Joint Publication 3-12

Joint Cyberspace Operations

19 December 2022

PREFACE

1. Scope

This publication provides joint doctrine to plan, execute, and assess cyberspace operations.

2. Purpose

This publication has been prepared under the direction of the Chairman of the Joint Chiefs of Staff (CJCS). It sets forth joint doctrine to govern the activities and performance of the Armed Forces of the United States in joint operations, and it provides considerations for military interaction with governmental and nongovernmental agencies, multinational forces, and other interorganizational partners. It provides military guidance for the exercise of authority by combatant commanders and other joint force commanders (JFCs) and prescribes joint doctrine for operations and training. It provides military guidance for use by the Armed Forces of the United States in preparing and executing their plans and orders. It is not the intent of this publication to restrict the authority of the JFC from organizing the force and executing the mission in a manner the JFC deems most appropriate to ensure unity of effort in the achievement of objectives.

3. Application

a. Joint doctrine established in this publication applies to the Joint Staff, combatant commands, subordinate unified commands, joint task forces, subordinate components of these commands, the Services, the National Guard Bureau, and combat support agencies.

b. This doctrine constitutes official advice concerning the enclosed subject matter; however, the judgment of the commander is paramount in all situations.

c. If conflicts arise between the contents of this publication and the contents of Service publications, this publication will take precedence unless the CJCS, normally in coordination with the other members of the Joint Chiefs of Staff, has provided more current and specific guidance. Commanders of forces operating as part of a multinational (alliance or coalition) military command should follow multinational doctrine and procedures ratified by the United States. For doctrine and procedures not ratified by the United States, commanders should evaluate and follow the multinational command's doctrine and procedures, where applicable and consistent with United States law, regulations, and doctrine.

For the Chairman of the Joint Chiefs of Staff:

Dagvin R.M. Anderson

DAGVIN R.M. ANDERSON
Lieutenant General, USAF
Director, Joint Force Development

Intentionally Blank

SUMMARY OF CHANGES
REVISION OF JOINT PUBLICATION 3-12
DATED 08 JUNE 2018

- **Changes title to "Joint Cyberspace Operations."**

- **Reflects change to a single command and control (C2) model vice having routine and crisis models.**

- **New C2 model reflects the Joint Force Headquarter-Cyberspace as the single point for all support to combatant commands (except United States Transportation Command, assigned to Joint Force Headquarters-Department of Defense Information Network).**

- **Reflects Cyber Mission Force use of joint task forces.**

- **Adds cyberspace system operation as a Department of Defense information network operations-related action distinct from cyberspace security actions.**

- **Reflects United States Cyber Command's updated *Unified Command Plan* responsibilities.**

- **Changes satellite communications references from United States Strategic Command to United States Space Command.**

- **Expands discussion of the law of war as applied to cyberspace attack.**

- **Adds more detailed discussion of the synchronization of offensive and defensive cyberspace operations (CO) and of internal and external CO missions.**

- **Defines new term "expeditionary cyberspace operations."**

- **Discusses new concepts of persistent engagement in cyberspace, defending forward in cyberspace, hunt forward operations, and mission-relevant terrain in cyberspace.**

- **Describes the concepts of global integration and the competition continuum as related to CO.**

Intentionally Blank

TABLE OF CONTENTS

APPENDIX

GLOSSARY

FIGURE

EXECUTIVE SUMMARY
COMMANDER'S OVERVIEW

- **Provides an overview of cyberspace and cyberspace operations**
- **Discusses cyberspace operations core activities**
- **Presents the Department of Defense authorities, roles, and responsibilities to shape cyberspace and provide integrated offensive and defensive options for the defense of the nation**
- **Discusses how to plan, coordinate, execute, and assess cyberspace operations**

Overview of Cyberspace and Cyberspace Operations

Introduction

Most aspects of joint operations rely in part on cyberspace, which is a global domain within the information environment (IE) that consists of the interdependent network of information technology (IT) infrastructures and resident data. It includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Cyberspace operations (CO) are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. A cyberspace capability is a device or computer program, including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace.

The Nature of Cyberspace

Relationship with the Physical Domains. Cyberspace, while part of the IE, is dependent on each of the physical domains. Much as operations in the physical domains rely on human-made infrastructure and naturally occurring features, operations in cyberspace rely on networked, stand-alone, and platform-embedded IT infrastructure, in addition to the data that resides on and is transmitted through these components, to enable military operations in a human-made domain. CO use links and nodes located in the physical domains and perform logical functions to create effects first in cyberspace and then, as needed, in the physical domains.

Cyberspace Layer Model. To assist in the planning and execution of CO, cyberspace can be described in terms of three interrelated layers: physical network, logical network, and cyber-persona. Each layer represents a different focus from which CO may be planned, conducted, and assessed.

Viewing Cyberspace Based on Location and Ownership. Maneuver in cyberspace is complex and generally not observable. Therefore, staffs that plan, execute, and assess CO benefit from language that describes cyberspace based on location or ownership in a way that aids rapid understanding of planned operations and required authorities.

Department of Defense (DOD) Cyberspace. The Department of Defense information network (DODIN) is the set of DOD-owned and DOD-leased information capabilities and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone.

Connectivity and Access. Cyberspace consists of myriad different and often overlapping elements, including networks, data centers, nodes, links, interrelated applications, user data, and system data.

The Operational Environment (OE). The OE is a composite of the conditions, circumstances, and influences that affect the employment of capabilities and impact the decisions of the commander. Understanding the relationship of cyberspace to the physical domains, the rest of the IE, and other elements of the OE is essential for planning military CO. The IE permeates the physical domains and, therefore, exists in any OE.

The IE. The IE is the aggregate of social, cultural, linguistic, psychological, technical, and physical factors that affect how humans and automated systems derive meaning from, act upon, and are impacted by information, including the individuals, organizations, and systems that collect, process, disseminate, or use information. It is an intellectual framework to help identify, understand, and describe how those often-intangible factors may affect the employment of forces and bear on the decision of the commander.

The Relationship of CO to Operations in the Information Environment (OIE). OIE combines CO with other information activities and capabilities to create effects in support of joint operations throughout the OE. Cyberspace is a domain through which other information activities and capabilities may operate. These activities and capabilities include, but are not limited to, military information support operations, military deception, public affairs, civil affairs, key leader engagement, and civil-military operations. CO can be conducted independently or synchronized, integrated, and deconflicted with other information capabilities and activities for more effective OIE.

Integrating Cyberspace Operations with Other Operations

During joint planning, CO are integrated into the joint force commander's (JFC's) plans, using the Chairman of the Joint Chiefs of Staff (CJCS)-directed global integration process, and synchronized with other operations across the competition continuum. This integration enables complex, globally integrated operations that are coordinated around the world at the speed of conflict and results in a more effective and lethal fighting force. While not the norm, some military objectives can be achieved by CO alone. In crisis and conflict, commanders conduct CO to obtain or retain freedom of maneuver in cyberspace, achieve JFC objectives, deny freedom of action to the threat, and enable other operational activities.

Cyberspace Forces

United States Cyber Command (USCYBERCOM) accomplishes its missions by conducting global campaigns along three primary lines of operation: secure, operate, and defend the DODIN; defend the nation from attack in cyberspace; and provide cyberspace support as required to combatant commanders (CCDRs). To enable this, the *(U) Global Force Management Implementation Guidance* assigns the preponderance of cyberspace forces to Commander, United States Cyber Command (CDRUSCYBERCOM). In accordance with (IAW) the *Unified Command Plan,* CDRUSCYBERCOM is designated as the CO joint force provider responsible for identifying and recommending global joint sourcing solutions to the CJCS, in coordination with the Services and other combatant commands (CCMDs), and supervising the implementation of sourcing decisions.

Challenges to the Joint Force's Use of Cyberspace

The JFC faces a unique set of persistent challenges executing CO and other operations in a constantly evolving, complex, and volatile global security environment characterized by contested norms of behavior in cyberspace and persistent disorder. To address these challenges, the JFC integrates CO with operations in all domains to support the DOD and CJCS global integration processes.

Threats. Cyberspace threats originate from states and their surrogates, criminal enterprises, individuals, and accidents and natural hazards, which together create a persistently contested environment in which the joint force plans and executes joint operations.

Geographic Challenges. Unlike the physical domains, cyberspace has no stateless maneuver space; it is all owned by someone. Therefore, when United States (US) military forces maneuver in gray and red cyberspace, mission and policy requirements may require clandestine maneuver, without the knowledge of the state where the infrastructure is located.

Technology Challenges. Using a cyberspace capability that relies on exploitation of technical vulnerabilities in the target may reveal its functionality and compromise the capability's effectiveness for future missions. This has implications for both external missions in gray and red cyberspace and internal missions in blue cyberspace.

Private Industry and Public Infrastructure. Many of DOD's critical functions and operations rely on contracted commercial assets, including Internet service providers and global supply chains, over which DOD and its forces have no direct authority. This includes both data storage services and applications provided from a cloud computing architecture.

Cyberspace Operations Core Activities

Introduction

CO are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. CO comprise the military, national intelligence, and ordinary business operations of DOD in and through cyberspace and are leveraged in support of each of the joint functions.

Military Operations In and Through Cyberspace

Cyberspace Missions. All actions in cyberspace that are not simply cyberspace-enabled activities are taken as part of one of three cyberspace missions: DODIN operations, defensive cyberspace operations (DCO), or offensive cyberspace operations (OCO). These three mission types, conducted under various sources of authority, comprehensively cover the activities of the cyberspace forces.

Cyberspace Actions. Execution of any DODIN operations, DCO, or OCO mission requires completion of specific actions that employ cyberspace capabilities to create effects in cyberspace. All cyberspace mission objectives are achieved by the combination of one or more of five cyberspace actions, which are defined exclusively by the types of effects they create.

Assignment of Cyberspace Forces to CO. Mission orders or other directives assign cyberspace forces to specific cyberspace missions.

Referring to Cyberspace Capabilities. Since capabilities are normally categorized by the types of effects they create, cyberspace capabilities are categorized by the cyberspace actions, not the cyberspace missions, which may have objectives that are too broad to be associated with a specific type of effect. Therefore, the most basic categories of cyberspace capabilities used on-net are: system operation, security, defense, exploitation, and attack.

Referring to Adversary Activities in Cyberspace. The DOD CO mission labels of DODIN operations, DCO, and OCO are selected based on commander's objectives and intent and, therefore, may not accurately describe the actions of our adversaries and enemies in cyberspace, whose mission objectives and commander's intent are usually not known with certainty. Therefore, the term "malicious cyberspace activity" (MCA) refers generally to all adversary and enemy cyberspace threat activities.

National Intelligence Operations In and Through Cyberspace

National-level intelligence organizations conduct intelligence activities in, through, and about cyberspace in response to national intelligence priorities. This intelligence supports military commanders' decision making and planning.

Department of Defense Ordinary Business Operations In and Through Cyberspace

Ordinary business operations in and through cyberspace are cyberspace-enabled activities that comprise those non-intelligence and non-warfighting capabilities, functions, and actions used to support and sustain DOD forces and components. This includes the cyberspace-enabled functions of the many civilian-run DOD agencies and activities, such as the Defense Finance and Accounting Service and the Defense Contract Audit Agency.

The Joint Functions and Cyberspace Operations

Command and Control (C2). Discussion of C2 and cyberspace requires a distinction between using IT systems that implement the C2 of all military operations and the C2 of forces that execute CO.

Use of cyberspace as a means of exchanging communications is overwhelmingly the most common method at the strategic and operational levels of warfare and is increasingly important in tactical warfare.

Intelligence. Understanding the OE is fundamental to all joint operations, including CO. Intelligence may be derived from information gained during military operations in cyberspace or from other sources.

Fires. Cyberspace attack capabilities create fires in and through cyberspace and are often employed with little or no associated physical destruction. However, modification or destruction of computers that control physical processes can lead to cascading effects (including collateral effects) in the physical domains. Depending upon the commander's objective, fires in cyberspace can be offensive or defensive, supporting or supported.

Movement and Maneuver. Movement and maneuver involves deploying forces and capabilities into an operational area and positioning within that area to gain operational advantage in support of mission objectives, including accessing and, as necessary, controlling key terrain. Standardizing the organization and force structure of the units of the Cyber Mission Force (CMF) and other cyberspace forces enhances their ability to maneuver in cyberspace, including deployment for expeditionary CO when necessary, although some CO can enable force projection without the need to establish a physical presence in foreign territory.

Sustainment. Sustainment is the provision of logistics and personnel services to maintain operations through mission accomplishment and redeployment of the force. From the perspective of cyberspace-enabled activities in support of global logistics, DOD relies on protected DODIN and commercial network segments to coordinate sustainment of forces.

Protection. Protection of the DODIN and other critical US cyberspace includes the continuous and synchronized integration of cyberspace security and, when required, cyberspace defense actions. Protection of cyberspace assets is complicated by their logical connectivity that can enable enemies to create multiple, cascading effects that may not be restricted by physical geography and civil/military boundaries.

Authorities, Roles, and Responsibilities

Introduction

Under the authorities of the Secretary of Defense (SecDef), DOD uses cyberspace capabilities to shape cyberspace and provide integrated offensive and defensive options for the defense of the nation. USCYBERCOM coordinates with CCMDs, the Joint Staff, and the Office of the Secretary of Defense; liaises with other United States Government (USG) departments and agencies; and, in conjunction with Department of Homeland Security (DHS), Department of Defense Cyber Crime Center (DC3), and the Defense Counterintelligence and Security Agency, liaises with members of the defense industrial base (DIB). Similarly, as directed, DOD deploys necessary resources to support efforts of other USG departments, as well as agencies and allies.

Authorities

Authority for CO actions undertaken by the Armed Forces of the United States is derived from the United States Constitution and federal law. Key laws that apply to DOD include Title 10, United States Code (USC); Title 50, USC; and Title 32, USC.

Roles and Responsibilities

SecDef. Directs the military, intelligence, and ordinary business operations of DOD in cyberspace.

Service Chiefs. Provide appropriate administration of and support to cyberspace forces, including units of the CMF, Service-retained forces, and forces assigned or attached to CCMDs.

Chief, National Guard Bureau. Advises the CJCS and CDRUSCYBERCOM on National Guard matters pertaining to CCMD CO missions and supports planning and coordination for such activities as requested by the CJCS or the CCDRs.

CDRUSCYBERCOM. Plans and executes global CO as directed.

Other CCDRs. Secure, operate, and defend tactical and constructed DODIN segments within their commands and areas of responsibility.

Director, Defense Information Systems Agency (DISA). Complies with CDRUSCYBERCOM direction, issued by the commander of Joint Force Headquarters-Department of Defense Information Network under delegated directive authority for cyberspace operations, to execute DODIN operations and defensive cyberspace operations-internal defensive measures missions at the global and enterprise level, within DISA-operated portions of the DODIN.

Director, National Security Agency/Chief, Central Security Service. Provides signals intelligence to national policy makers and military forces; cybersecurity policy guidance and assistance to DOD components, DIB, and national customers; and technical support, including encryption and cross-domain network solutions.

Director, DC3. Administratively assigned to the Department of the Air Force but supporting the entire DOD, the DC3 provides digital and multimedia forensics; cybersecurity incident investigative and technical training; technical solutions research, development, test, and evaluation; critical infrastructure protection; and cyberspace vulnerability analysis for DODIN protection, law enforcement (LE), intelligence community, counterintelligence (CI), and counterterrorism organizations.

Other DOD Agencies and Activities. All DOD agencies and activities are responsible for developing, maintaining, and operating their IT in a manner consistent with and reflective of applicable DODIN architecture and cybersecurity policy standards, and they plan, resource, acquire, implement, and maintain agency-specific IT IAW DOD policy and resource priorities.

DHS. Secures US cyberspace, at the national level, by protecting non-DOD USG networks against cyberspace exploitation and attacks, including actions to reduce and consolidate external access points, deploy passive network defenses and sensors, and define public and private partnerships in support of national cybersecurity policy.

Department of Justice (DOJ). DOJ, including the Federal Bureau of Investigation, leads counterterrorism and CI investigations and related LE activities associated with government and commercial critical infrastructure and key resources (CI/KR). DOJ investigates, defeats, prosecutes, and otherwise reduces foreign intelligence, terrorist, and other cyberspace threats to the nation's CI/KR.

Legal Considerations

DOD conducts CO in compliance with US domestic law, applicable international law, and relevant USG and DOD policies. Laws applicable to military activities in the United States also apply to cyberspace. DOD cyberspace forces generally operate either on the DODIN or, when properly authorized, in gray and red cyberspace, or other blue cyberspace, when, for example, conducting hunt forward operations or defense support of civil authorities under appropriate authority. Each CO mission has unique legal considerations. Before conducting CO, commanders, planners, and operators require clear understanding of the relevant legal framework to ensure compliance with laws and policies. It is essential commanders, planners, and operators consult with legal counsel during planning and execution of CO.

Planning, Coordination, Execution, and Assessment

Joint Planning Process and Cyberspace Operations

Commanders integrate CO into their campaigns and operations at all levels. Their plans should address how to effectively integrate cyberspace capabilities, counter adversaries' use of cyberspace, identify and secure mission-relevant terrain in cyberspace, access key terrain in cyberspace, operate in a denied environment, efficiently use limited cyberspace assets, and pair operational requirements with cyberspace capabilities.

CDRUSCYBERCOM plans, executes, and assesses CO based on a strategy of persistent engagement in cyberspace, employing a continuous operational tempo to seize and maintain the initiative required to compete and to set favorable security conditions in and through the IE that secure, defend, and advance US strategic goals.

Cyberspace Operations Planning Considerations

Although CO planners are presented the same operational design considerations and challenges as planners for operations in the physical domains, there are some unique considerations for planning CO. For instance, because of unforeseen linkages in cyberspace, higher-order effects of some CO external missions may be difficult to predict. This may require extensive branch and sequel planning. Further, while many elements of cyberspace can be mapped geographically, a full understanding of an adversary's disposition and capabilities in cyberspace involves understanding the target, not only at the underlying physical network layer but also at the logical network layer and cyber-persona layer, including profiles of system users and administrators and their relationship to adversary critical factors.

Intelligence and Operational Analytic Support to Cyberspace Operations Planning

During mission analysis, the joint force staff identifies priority intelligence requirements (PIRs) about the threat and other relevant aspects of the OE. Based upon the PIRs, the intelligence staff develops more specific essential elements of information, indicators, and specific information requirements to inform CCDR decision making. Information requirements related to cyberspace can include such things as network infrastructures and status, readiness of the threat's equipment and personnel, and unique cyberspace signature identifiers such as hardware/software/

firmware versions and configuration files. The resulting requirements are met through a combination of military intelligence and national intelligence sources, including open sources.

Joint Targeting

Joint Targeting In and Through Cyberspace. Planning and targeting staffs develop and select targets in and through cyberspace based on the commander's objectives rather than on the capabilities available to achieve them. The focus is on creating effects that accomplish targeting-related tasks and that support achievements of objectives, not on using a particular cyberspace capability simply because it is available. Targets that can be accessed in cyberspace are developed, vetted, and validated within the established joint targeting process.

Command and Control of Cyberspace Forces

Clearly established command relationships are crucial for ensuring timely and effective employment of forces, and CO require unity of command and unity of effort. However, the complex nature of CO, where cyberspace forces can be simultaneously providing actions at the global level and at the theater or joint operations area level, requires adaptive C2 structures. Joint forces principally employ centralized planning with decentralized execution of operations. CO require constant and detailed coordination between theater and global operations, creating a dynamic C2 framework that can adapt to the constant changes, emerging threats, and unknowns. Certain CO functions, including protection of the DODIN against global cyberspace threats, lend themselves to centralized planning and execution to meet multiple, near-instantaneous requirements for response.

Synchronization of Cyberspace Operations

The pace of CO requires significant pre-operational collaboration and constant vigilance after initiation, for effective coordination and deconfliction throughout the OE. Keys to this synchronization are maintaining cyberspace situational awareness and assessing the potential impacts to the joint force of any planned CO, including the protection posture of the DODIN, changes from normal network configuration, or observed indications of MCA. The timing of planned CO should be determined based on a realistic assessment of their ability to create effects and support operations throughout the OE.

Assessment of Cyberspace Operations

Assessment measures progress of the joint force toward mission accomplishment. Commanders continuously assess the OE and the progress of CO and compare them to their vision and intent. Measuring this progress toward the end state, and delivering timely, relevant, and reliable feedback into the planning process to adjust operations during execution, involves deliberately comparing the forecasted effects of CO with actual outcomes to determine the overall effectiveness of cyberspace force employment.

Interorganizational Considerations

When appropriate, JFCs coordinate and integrate their CO with interagency partners during planning and execution. Effective integration of interagency considerations is vital to successful military operations, especially when the joint force conducts shaping, stabilization, and transition to civil authority activities. Just as JFCs and their staffs consider how the capabilities of other USG departments and agencies and nongovernmental organizations can assist in accomplishing military missions and achieving broader national strategic objectives, JFCs should also consider the capabilities and priorities of interagency partners in planning and executing CO.

Multinational Considerations

Collective security is a strategic objective of the United States, and joint planning is frequently accomplished within the context of planning for multinational operations. Despite the potential for increased risk inherent in relying on others, the complexity of cyberspace and the enormous variety of its threats means the United States does rely on partnerships to protect its cyberspace and to achieve CO external mission objectives. There is no single doctrine for multinational action, and each alliance or coalition develops its own protocols and plans. US planning for joint operations accommodates and complements such protocols and plans for potential use of US cyberspace forces to protect multinational force networks.

CONCLUSION

This publication provides joint doctrine to plan, execute, and assess CO.

CHAPTER I
OVERVIEW OF CYBERSPACE AND CYBERSPACE OPERATIONS

1. Introduction

a. Most aspects of joint operations rely in part on cyberspace, which is a global domain within the information environment (IE) that consists of the interdependent network of information technology (IT) infrastructures and resident data. It includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Cyberspace operations (CO) are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. A cyberspace capability is a device or computer program, including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace.

b. This publication focuses on military operations in and through cyberspace; explains the relationships and responsibilities of the Joint Staff (JS); combatant commands (CCMDs), including United States Cyber Command (USCYBERCOM) and its Service cyberspace component (SCC) commands; and combat support agencies (CSAs) and establishes a globally integrated framework for the employment of cyberspace forces. Cyberspace forces are those personnel whose primary duty assignment is to a CO mission.

c. **The Impact of Cyberspace on Joint Operations**

(1) CO provide opportunities for the United States (US), its allies, and partner nations (PNs) to gain and maintain continuing advantages in the operational environment (OE) and enable the nation's economic and physical security. Cyberspace reaches across geographic and geopolitical boundaries and is integrated with the operation of critical infrastructures, as well as the conduct of commerce, governance, and national defense activities. Access to the Internet and other areas of cyberspace provides users operational reach and malign actors the opportunity to compromise the integrity of critical infrastructures in direct and indirect ways without a physical presence. The prosperity and security of our nation are significantly enhanced by our use of cyberspace. Yet technological developments create a critical dependence on this domain and increase exposure to vulnerabilities in cyberspace, for the United States in general and the joint force in particular.

(2) CO integrated with operations in other domains create coordinated and synchronized effects required to support mission accomplishment; however, CO may also be used to produce stand-alone tactical, operational, or strategic effects to achieve objectives. The mission assurance of CCMDs and other Department of Defense (DOD) components, along with the core functions of the federal, state, local, territorial, and tribal governments and the same components of our allies and PNs, depend on cyberspace-enabled capabilities and the information that resides in cyberspace.

(3) Permanent global cyberspace superiority is impossible due to the complexity of cyberspace. Even local superiority may be impractical due to the way IT is

implemented; the fact that the United States and most other nations do not directly control large, privately owned portions of cyberspace; the broad array of state and non-state actors; the low cost of entry; and the rapid and unpredictable proliferation of technology. Therefore, commanders should prepare to conduct operations under degraded conditions in cyberspace. However, once one segment of cyberspace is exploited or denied, a joint force commander (JFC) may incorrectly perceive that the associated risk extends beyond the compromised segment due to the uncertainty about how networks interact. Therefore, it is imperative commanders be well-informed of the status of the portions of cyberspace upon which they depend and understand the impact of potential cyberspace threats to planned and ongoing operations.

2. The Nature of Cyberspace

a. **Relationship with the Physical Domains.** Cyberspace, while part of the IE, is dependent on each of the physical domains. Much as operations in the physical domains rely on human-made infrastructure and naturally occurring features, operations in cyberspace rely on networked, stand-alone, and platform-embedded IT infrastructure, in addition to the data that resides on and is transmitted through these components, to enable military operations in a human-made domain. CO use links and nodes located in the physical domains and perform logical functions to create effects first in cyberspace and then, as needed, in the physical domains. Critical links and nodes are identified by planners for increased protection, including physical security when necessary, to ensure freedom of maneuver in both cyberspace and the physical domains. Effects are the results, outcomes, consequences, and state changes resulting from an action. Cyberspace actions detailed in Chapter II, “Cyberspace Operations Core Activities,” are defined based on the types of effects they create in cyberspace. Some cyberspace actions, carefully controlled to create cascading effects, can enable lethal and nonlethal effects in the physical domains. Likewise, activities in the physical domains can create effects in and through cyberspace by affecting the physical infrastructure or the portions of the electromagnetic spectrum (EMS) that enable CO. The relationship between the space domain and cyberspace is unique. Virtually all space operations depend on cyberspace, and a critical portion of cyberspace bandwidth can be provided only via space operations, which provide a key global connectivity option for CO. These interrelationships are important considerations during planning. While domains are useful constructs for visualizing and characterizing the physical environment in which operations are conducted (i.e., the operational area [OA]), the use of the term “domain” is not meant to imply or mandate exclusivity, primacy, or command and control (C2) authority in any domain.

b. **Cyberspace Layer Model.** To assist in the planning and execution of CO, cyberspace can be described in terms of three interrelated layers: physical network, logical network, and cyber-persona (see Figure I-1). Each layer represents a different focus from which CO may be planned, conducted, and assessed.

(1) The **physical network layer** consists of the IT devices and infrastructure in the physical domains that provide storage, transport, and processing of information within cyberspace, to include data repositories and the connections that transfer data between network components. The physical network components include the hardware and

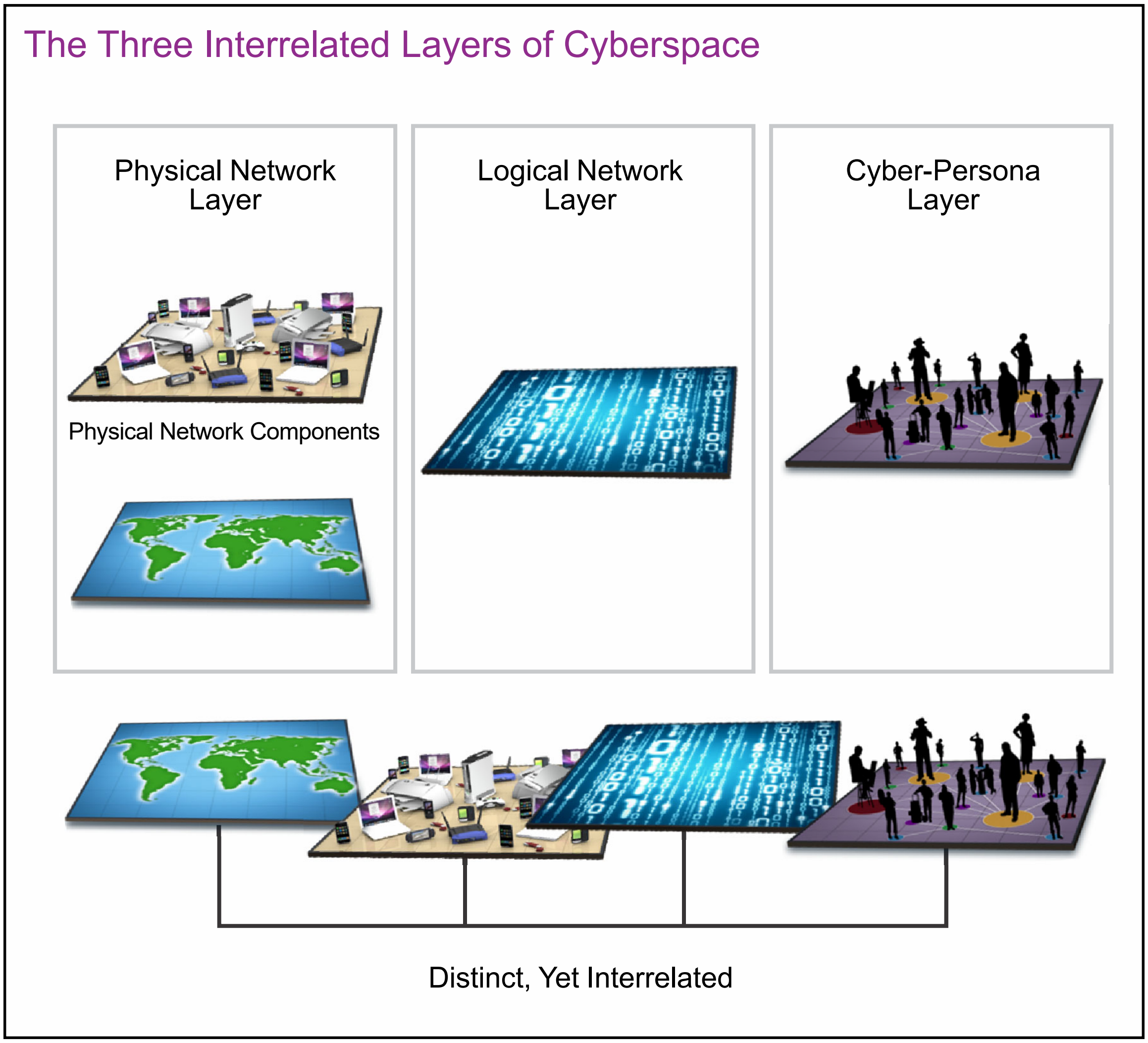

The Three Interrelated Layers of Cyberspace
Physical Network Layer
Logical Network Layer
Cyber-Persona Layer
Physical Network Components
Distinct, Yet Interrelated

Figure I-1. The Three Interrelated Layers of Cyberspace

infrastructure (e.g., computing devices, storage devices, network devices, and wired and wireless links). Physical access to these devices can present significant freedom of action against targets in cyberspace. Therefore, components of the physical network layer require physical security measures to protect them from physical damage or unauthorized physical access, which can sometimes be leveraged to gain logical access. The physical network layer is the first point of reference CO use to determine geographic location and appropriate legal framework. While geopolitical boundaries can easily and quickly be crossed in cyberspace, crossing these boundaries involves the principle of territorial sovereignty tied to the physical domains. Every physical component of cyberspace is owned by a public or private entity, which can control or restrict access to its components. These unique characteristics of the OE inform all phases of planning.

(2) The **logical network layer** consists of those elements of the network related to one another in a way that is abstracted from the physical network, based on the logic programming (code) that drives network components (i.e., the relationships are not necessarily tied to a specific physical link or node but to their ability to be addressed

logically and exchange or process data). Individual links and nodes are represented in the logical layer, but various distributed elements of cyberspace, including data, applications, and network processes, are not tied to a single node. An example is the Joint Knowledge Online website, which exists on multiple servers in multiple locations in the physical domains but is represented as a single URL [uniform resource locator] on the World Wide Web. More complex examples of the logical layer are DOD's Nonclassified Internet Protocol Router Network (NIPRNET) and SECRET Internet Protocol Router Network (SIPRNET), which are global, multi-segment networks that can be thought of as a single network only in the logical sense. There are things with intrinsic value that exist only in the logical layer, such as digital currency, non-fungible tokens, or a retirement savings account. Such logical entities may be valid joint targets. For joint targeting purposes, planners may know the logical location of some targets, such as virtual machines and operating systems, that allow multiple servers or other network functions with separate Internet protocol (IP) addresses to reside on one physical computer, without knowing their geographic location. Logical layer targets can only be directly engaged with a cyberspace capability.

(3) The **cyber-persona layer** is a view of cyberspace created by abstracting and combining data from the logical network layer to develop descriptions of digital representations of an actor or entity identity in cyberspace (cyber-persona). The cyber-persona layer consists of network or IT user accounts, whether human or automated, and their relationships to one another. Cyber-personas may relate directly to an actual person or entity, incorporating some personal or organizational data (e.g., e-mail and IP addresses, websites, phone numbers, Web forum logins, or financial account passwords). One individual may create and maintain multiple cyber-personas through use of multiple identifiers in cyberspace, such as separate work and personal e-mail addresses, and different identities on different Web forums, chat rooms, and social networking sites, which may vary in the degree to which they are factually accurate. Conversely, a single cyber-persona can have multiple users, such as multiple hackers using the same malicious software (malware) control alias, multiple extremists using a single bank account, or all members of the same organization using the same e-mail address. The use of cyber-personas can make attributing responsibility for actions in cyberspace difficult. However, cyber-personas operate on IT infrastructure in the physical network layer and a combination of programming code and data in the logical network layer. Analysis of artifacts from all three layers can enable attribution and, when authorized, effective joint targeting. Because cyber-personas can be complex, with elements in many virtual locations not linked to a single physical location or form, their identification requires significant intelligence collection and analysis to provide enough insight and situational awareness to enable effective joint targeting or to create the JFC's desired effect. Like the logical network layer, complex changes to cyber-personas can happen very quickly compared to similar changes in the physical network layer, complicating actions against these targets without detailed change tracking.

c. **Viewing Cyberspace Based on Location and Ownership.** Maneuver in cyberspace is complex and generally not observable. Therefore, staffs that plan, execute, and assess CO benefit from language that describes cyberspace based on location or ownership in a way that aids rapid understanding of planned operations and required authorities. The term “blue cyberspace” denotes US cyberspace (i.e., areas in cyberspace owned or controlled by the United States Government [USG] or a US person) and other areas of cyberspace DOD is ordered to protect. This can include allied or PN cyberspace, which is temporarily considered blue cyberspace for the duration of the ordered protection activity. Although DOD has standing orders to protect only the Department of Defense information network (DODIN), cyberspace forces prepare, on order, to defend USG or other blue cyberspace, including cyberspace related to critical infrastructure and key resources (CI/KR) of the United States and PNs. The term “red cyberspace” refers to those portions of cyberspace owned or controlled by, or on behalf of, an adversary or enemy. In this case, “controlled” means more than simply “having a presence on,” since threats may have clandestine access to elements of cyberspace where their presence is undetected and without apparent impact to the operation of the system. Here, “controlled” means the ability to direct the operations of a link or node of cyberspace, to the exclusion of others. All cyberspace that does not meet the description of either “blue” or “red” is referred to as “gray cyberspace.” Information provided by interagency, industry, and international partners may facilitate greater situational awareness of location and ownership issues.

d. **DOD Cyberspace.** The DODIN is the set of DOD-owned and DOD-leased information capabilities and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, whether interconnected or stand-alone. This includes communications and computing systems and services, software, data, security services, other associated services, and national security systems. The DODIN comprises all of DOD cyberspace, including the classified and unclassified global networks (e.g., NIPRNET, SIPRNET, Joint Worldwide Intelligence Communications System) and many other components. The DODIN includes common enterprise service networks, intelligence networks operated by DOD components, stand-alone mission and weapon systems, other special-purpose networks, DOD-owned smartphones, radio frequency identification tags, industrial control systems, isolated laboratory networks, and platform information technology (PIT) operated by or on behalf of DOD components. PIT is the hardware and software that is physically part of, dedicated to, or essential in real time to the mission performance of special-purpose systems, including weapon systems. DOD also increasingly relies on commercial and government “cloud” services for on-demand data processing, data storage, and application hosting provided over the Internet, without active management by the DOD user. Nearly every military and civilian employee of DOD uses the DODIN to accomplish some portion of their mission or duties. To enable unity of action for DODIN protection, USCYBERCOM divides the DODIN into areas of operations in which joint or Service commanders and agency and field activity directors maintain accountability over cyberspace assigned to them and into sectors that overlap the areas of operations to group portions of the DODIN based on the missions and functions they serve.

e. **Connectivity and Access.** Cyberspace consists of myriad different and often overlapping elements, including networks, data centers, nodes, links, interrelated applications, user data, and system data. It is estimated that over 100 new devices are connected to the Internet every second, including PIT in devices like home appliances, remote sensors, and vehicles and other things whose users may not necessarily understand are on-line. Such devices are referred to as the "Internet of Things" (IoT). The existence of a very rapidly expanding IoT creates both advantages for accessing targets from within cyberspace and disadvantages of congested bandwidth, greater security risks, and an increasingly complex terrain for maneuver. Even though cyberspace continues to become increasingly interconnected, some elements are intentionally isolated or subdivided into enclaves using access controls, encryption, unique protocols, or physical separation. With the exception of actual physical isolation, none of these approaches eliminate the underlying physical connectivity; instead, they limit access to the logical network. Access, whether authorized or unauthorized, is gained through a variety of means. Although CO require timely and effective connectivity and access, the USG may not own, control, or have access to the infrastructure needed to support a specific US military operation. For CO, access means a sufficient level of exposure to, connectivity to, or entry into a device, system, or network to achieve the objective. While some accesses can be created remotely, with or without permission of the network owner, access to closed networks and other systems that are virtually isolated may require physical proximity or more complex, time-consuming processes, such as expeditionary CO. In addition, gaining access to operationally useful areas of cyberspace, including targets within them, is affected by legal, policy, or operational limitations. For all of these reasons, access is not guaranteed. Additionally, achieving a commander's objectives can be significantly complicated by specific elements of cyberspace being used simultaneously by enemies, adversaries, allies, neutral parties, and other USG departments and agencies. Therefore, synchronization and deconfliction of CO access is critical to successful operations of all types.

f. **The OE.** The OE is a composite of the conditions, circumstances, and influences that affect the employment of capabilities and impact the decisions of the commander. Understanding the relationship of cyberspace to the physical domains, the rest of the IE, and other elements of the OE is essential for planning military CO. The IE permeates the physical domains and, therefore, exists in any OE. The continuing advancement of IT, including the IoT, has significantly reduced its cost of acquisition and application, leading to the rapid proliferation of cyberspace capabilities and considerably complicating an already complex OE. For instance, CO from moving platforms require transmission through the EMS, which is significantly affected by congestion (i.e., interference from commercial and military use), atmospheric conditions, and enemy electromagnetic attack (EA). The decision to use CO to create effects may be affected by factors ranging from broad, national strategic objectives down to the requirement to affect a single individual's ability to use cyberspace.

(1) The IoT, including the pervasiveness of mobile IT, is forcing governments and militaries to re-evaluate the impact of the IE on operations. The nature of global social interaction has been changed by the rapid flow of information from around-the-clock news, including from nontraditional and unverifiable sources such as social networking, media sharing and broadcast sites, online gaming networks, topical forums, and text messaging. The popularity of these information sources enables unprecedented interaction among global populations, much of which is increasingly relevant to military operations. The ability of social networks in cyberspace to incite popular support and to spread ideology is

not geographically limited, and the continued proliferation of IT has profound implications for the joint force and US national security.

(2) State and non-state threats use a wide range of low-cost, advanced technologies, which represent an inexpensive way for a small and/or materially disadvantaged adversary to pose a significant threat to the United States. The application of low-cost cyberspace capabilities can provide an advantage against a technology-dependent nation or organization. This can provide an asymmetric advantage to those who could not otherwise effectively oppose US military forces. Additionally, organized crime or other non-state, extralegal organizations often make sophisticated malware available for purchase or free, allowing even non-sophisticated threats to acquire advanced capabilities at little to no cost. Due to the low barriers to entry and the potentially high payoff, the United States can expect an increasing number of adversaries to use cyberspace threats to attempt to negate US advantages in military capability. Adversaries may combine cyberspace attacks with malign influence efforts and/or lethal attacks to exploit their synergy.

(3) **Key terrain in cyberspace** is analogous to key terrain in the physical domains in that access to or control of it affords any combatant a position of marked advantage. In cyberspace, it may only be necessary to maintain a secure presence on a particular location or in a particular process as opposed to seizing and retaining it to the exclusion of all others. It is possible for the United States and an adversary to occupy the same terrain or use the same process in cyberspace, potentially without knowing of the other's presence. An additional characteristic of terrain in cyberspace is that these localities have a virtual component, identified in the logical network layer or even the cyber-persona layer. Key terrain identification is an essential component of planning. The military aspects of terrain (e.g., obstacles, avenues of approach [offensive and defensive], cover and concealment, observation and fields of fire, and key terrain) provide a way to visualize and describe a network or system map. Obstacles in cyberspace may include firewalls, blocked server ports, or active intrusion detection systems. Avenues of approach can be analyzed by identifying nodes and links, which connect endpoints to specific sites. Cover and concealment may refer to hidden IP addresses or password protected access. Cyberspace observation and fields of fire refer to areas where network traffic can be monitored, intercepted, or recorded. Examples of potential key terrain in cyberspace include access points to major lines of communications, key waypoints for observing incoming threats, launch points for cyberspace attacks, and mission-relevant terrain related to critical assets connected to the DODIN or other cyberspace. Operators, planners, and intelligence staff work together with CO planning staff to match plans' objectives with terrain analysis to determine key terrain in blue, gray, and red cyberspace for each plan. Correlating plan or mission objectives with key terrain ensures mission dependencies in cyberspace are identified and prioritized for protection (i.e., secured and defended) in a standard manner across DOD. In many cases, the systems, networks, and infrastructure that support a mission objective are interdependent. These complex interdependencies may require in-depth mission analysis to develop customized risk mitigation methodologies. Risk mitigation is not risk avoidance, and commanders make risk-informed decisions about use of key terrain in cyberspace that support mission accomplishment.

(4) **Mission-relevant terrain in cyberspace (MRT-C)** is another important CO planning construct. MRT-C is an element of the mission assurance process and it comprises the resources in cyberspace required to ensure the joint force can complete an assigned mission. It includes all devices, links, applications, services, and other technical aspects of a system, on or off the DODIN, required by that mission. Off-DODIN MRT-C is other publicly or privately owned cyberspace relied upon to perform DOD missions. Identifying MRT-C establishes a requirement to consider protecting that terrain to reduce mission risk and to plan for elevated mission risk when adequate protections of MRT-C are not possible. Since the terrain in cyberspace is constantly evolving, the MRT-C identification and mapping process is repeated periodically to ensure commanders have the most accurate information on which to base mission risk management decisions.

g. **The IE.** The IE is the aggregate of social, cultural, linguistic, psychological, technical, and physical factors that affect how humans and automated systems derive meaning from, act upon, and are impacted by information, including the individuals, organizations, and systems that collect, process, disseminate, or use information. It is an intellectual framework to help identify, understand, and describe how those often-intangible factors may affect the employment of forces and bear on the decision of the commander. Since all CO require the creation, processing, storage, and/or transmission of information, cyberspace is wholly contained within the IE, and CO are a form of information activity. The IE is broken down into the physical, informational, and cognitive dimensions and includes many types of information not in cyberspace. Although the types of information not processed within cyberspace continue to dwindle, there remain individuals and organizations that handle their information requirements outside of cyberspace, particularly when security, durability, cost, and scope factors are significant.

h. **The Relationship of CO to Operations in the Information Environment (OIE)**

(1) OIE can combine CO with other information activities and capabilities to create effects in support of joint operations throughout the OE. Cyberspace is a domain through which other information activities and capabilities may operate. These activities and capabilities include, but are not limited to, military information support operations (MISO), military deception (MILDEC), public affairs, civil affairs, key leader engagement, and civil-military operations. CO can be conducted independently or synchronized, integrated, and deconflicted with other information capabilities and activities for more effective OIE.

(2) While all CO impact the IE and are often designed, planned, and executed for effects specifically in the IE, commanders may conduct CO to support the full range of military objectives that are integrated globally using guidance from the Chairman of the Joint Chiefs of Staff (CJCS); Commander, United States Cyber Command (CDRUSCYBERCOM); and the supported combatant commander (CCDR). Failure to synchronize CO with planning and execution of other military operations, and with applicable intelligence community (IC) and law enforcement (LE) agencies, can result in friendly force interference and may counter the simplicity, agility, and economy of force principles of joint operations. This synchronization is particularly important during the transition between using intermediate force capabilities, including when lethal and nonlethal actions occur.

Refer to Joint Publication (JP) 3-0, Joint Campaigns and Operations; *JP 3-04,* Information in Joint Operations; *and JP 3-61,* Public Affairs, *for information on the primary activities that support the information joint function.*

3. Integrating Cyberspace Operations with Other Operations

a. During joint planning, CO are integrated into the JFC's plans, using the CJCS-directed global integration process, and synchronized with other operations across the competition continuum. This integration enables complex, globally integrated operations that are coordinated around the world at the speed of conflict and results in a more effective and lethal fighting force. While not the norm, some military objectives can be achieved by CO alone. In crisis and conflict, commanders conduct CO to obtain or retain freedom of maneuver in cyberspace, achieve JFC objectives, deny freedom of action to the threat, and enable other operational activities. In some cases, an adversary or situation may generate a threat across multiple CCDR geographic or functional areas. Planning an effective response to these threats requires global integration of CO within the context of multiple JFCs and numerous other DOD and USG activities. Response to such threats may require CO to be centrally executed to ensure required operational timing and tempo and to ensure globally deconflicted and synchronized actions. However, some CO require the deployment of personnel or units of cyberspace forces within the physical domains (decentralized execution) to interoperate with other forces or to gain access to cyberspace that cannot be accessed remotely. Maneuver forces conducting these expeditionary CO require specific planning, training, and often unique authorities and cyberspace capabilities and operate across the competition continuum at the tactical, operational, and strategic levels of warfare.

b. Issues that may need to be addressed to fully integrate CO into joint planning, execution, and assessment include centralized CO planning for DODIN operations; the JFC's need to integrate and synchronize all operations and fires across the entire OE, including the cyberspace aspects of joint targeting; deconfliction requirements between government entities; PN relationships; and the wide variety of authorities and legal issues related to the use of cyberspace capabilities. This requires all members of the commander's staff who conduct planning, execution, and assessment of operations to understand the fundamental processes and procedures for CO, including the organization and functions of assigned or supporting cyberspace forces.

c. Effective integration of CO with operations in the physical domains requires the active participation of CO planners and operators in each phase of joint operations on every staff supported by cyberspace forces. CO, especially when combined with intermediate force capabilities/integrating nonlethal and lethal options, can greatly enhance a commander's ability to accomplish the mission. Global integration of CO protects globally distributed warfighting platforms and networks and allows the joint force to engage threats that have established globally dispersed footprints in cyberspace. The physical and logical boundaries within which joint forces execute CO, and the priorities and restrictions on its use, should also be identified by planners, in coordination with other USG departments and agencies and national leadership. In particular, creation of effects in gray or red cyberspace may have the potential to impact other USG efforts. Where the potential for such impact exists, national policy requires DOD coordination with interagency partners.

d. **Network Engagement.** Using a network engagement approach to mission analysis can improve integration of CO with other operations. Network engagement is the JFC's interaction with friendly, neutral, and threat networks, conducted continuously and simultaneously at the tactical, operational, and strategic levels, to help achieve objectives within an OA. Network engagement includes planning approaches and network analytical tools, such as critical factors analysis and social network analysis, to clarify network relationships and dependencies. These techniques are often applied to human-based networks, such as found in the cyber-persona layer of cyberspace, but can also provide crucial insight into the relationship between the physical and logical networks in cyberspace and networks in the other domains. Network engagement is particularly important in operations that simultaneously involve friendly, neutral, and threat networks. When the joint force partners with friendly networks and conducts network engagement with neutral networks by building mutual trust and cooperation, it can aid in countering threats to all networks, including cyberspace threats. Globally integrated and unified network engagement action provides the opportunity for the JFC to create powerful friendly networks with far-reaching capabilities and to engage with neutral networks to either solicit their assistance or prevent them from supporting a threat network.

Refer to JP 3-25, Joint Countering Threat Networks, *for information on network engagement and network analysis tools.*

Refer to Chapter IV, "Planning, Coordination, Execution, and Assessment," for more information about planning, synchronization, integration, and interorganizational coordination of CO.

4. Cyberspace Forces

a. USCYBERCOM accomplishes its missions by conducting global campaigns along three primary lines of operation: secure, operate, and defend the DODIN; defend the nation from attack in cyberspace; and provide cyberspace support as required to CCDRs. To enable this, the *(U) Global Force Management Implementation Guidance* (GFMIG) assigns the preponderance of cyberspace forces to CDRUSCYBERCOM. In accordance with (IAW) the *Unified Command Plan,* CDRUSCYBERCOM is designated as the CO joint force provider responsible for identifying and recommending global joint sourcing solutions to the CJCS, in coordination with the Services and other CCMDs, and supervising the implementation of sourcing decisions. Secretary of Defense (SecDef) policy designates the elements of the Cyber Mission Force (CMF), certain CO units that conduct internal missions in blue cyberspace, and other specialized CO units as "cyberspace operations forces" for the purposes of joint force trainer responsibilities. The Services staff, train, and equip cyberspace units and provide them to USCYBERCOM through the SCCs. USCYBERCOM ensures cyberspace forces are sufficiently trained, certified, and interoperable to meet mission requirements. According to the *Memorandum of Agreement Between the Department of Defense and the Department of Homeland Security Regarding*

Department of Defense and US Coast Guard Cooperation on Cyberspace Security and Cyberspace Operations, the Commandant of the Coast Guard retains operational control (OPCON) of United States Coast Guard cyberspace forces when employed in support of DOD. As directed by SecDef, USCYBERCOM uses a mission alignment process to develop requirements-driven, risk-informed, CMF-alignment recommendations and tasking to assigned or attached cyberspace units to perform CO to achieve CCDR objectives.

b. **CMF.** SecDef and the CJCS established the CMF to organize and resource the force structure required to conduct key CO missions. CDRUSCYBERCOM exercises combatant command (command authority) (COCOM) of the CMF, which is a subset of DOD's total force for CO. Various Service tactical cyberspace units, assigned to CDRUSCYBERCOM, comprise the three elements of the CMF:

(1) **Cyber Protection Force (CPF).** The CPF conducts CO for internal defense of the DODIN or other blue cyberspace when ordered. The CPF consists of cyberspace protection teams (CPTs), which are organized, trained, and equipped to defend assigned cyberspace in coordination with and in support of system operators, local defenders, cybersecurity service providers (CSSPs), and users. CPTs are often the first to directly encounter threats in blue cyberspace and require significant intelligence support to stay threat-informed. When CSSPs and local defenders encounter threats in assigned cyberspace, they have the ability to reach back to supporting CPTs to stay threat-informed. For ease of reference, the CPTs are categorized and labeled as noted below based on the USCYBERCOM component to which they are OPCON and the parts of blue cyberspace they normally defend. However, all CPTs are assigned to USCYBERCOM and are available to CDRUSCYBERCOM to be aligned and/or deployed as required, based on the threat environment and the CPT's capability and capacity. All CPTs have similar baseline training and specialized assignment training, and they are tasked based on operational requirements and their availability. Each CPT is OPCON to a USCYBERCOM subordinate headquarters (HQ) and may be placed in direct support of a JFC when required. CPTs OPCON to a joint force headquarters-cyberspace (JFHQ-C) are normally employed in direct support of CCMD requirements. Similarly, CPTs OPCON to the SCCs support defense of Service cyberspace, CPTs OPCON to Joint Force Headquarters-Department of Defense Information Network (JFHQ-DODIN) normally defend non-Service portions of the DODIN, and CPTs OPCON to the Cyber National Mission Force-Headquarters (CNMF-HQ) primarily support defense of non-DODIN blue cyberspace.

(2) **Cyber National Mission Force (CNMF).** The CNMF conducts CO to defeat cyberspace threats to the DODIN and the nation. The CNMF comprises various numbered national mission teams (NMTs), associated national support teams (NSTs), and national CPTs focused on defense of non-DODIN blue cyberspace.

(3) **Cyber Combat Mission Force (CCMF).** The CCMF conducts CO to support the missions, plans, and priorities of the CCDRs. The CCMF comprises various numbered combat mission teams (CMTs) and associated combat support teams (CSTs)

c. **USCYBERCOM Subordinate Command Elements.** Subordinate HQs of USCYBERCOM execute C2 of the CMF and other cyberspace forces. These include the CNMF-HQ, the JFHQ-DODIN, four JFHQ-Cs, and the SCC HQs. Each of the SCC commanders is dual-hatted by CDRUSCYBERCOM as a commander of one of the four JFHQ-Cs to enable synchronization of joint CO with Service CO. In addition, there are other centers and staff elements that further enable unity of command for CO, including various joint task forces (JTFs) established by CDRUSCYBERCOM or subordinate commanders as required. The functional diagram in Figure I-2 portrays the general organization of the CMF and the source of guidance for its teams. There are exceptions to these relationships when required for efficiency and economy of force. For example, the CCMD CPT support for United States Transportation Command is provided by CPTs OPCON to JFHQ-DODIN. Chapter III, "Authorities, Roles, and Responsibilities," contains more detailed descriptions of these subordinate command responsibilities and the related C2 relationships.

d. **Other Cyberspace Forces and Staff.** Most cyberspace forces that operate and protect the DODIN are Service-retained and some are employed in support of a specific CCDR. They may be employed by the Service or SCCs both to operationalize networks (i.e., design, build, configure, and otherwise prepare to place into operation) and then secure, operate, and defend their Service-provisioned components of the DODIN. The Services may retain, or other CCDRs may organize, other specialized cyberspace forces that support CCMD missions as required. Some of these Service-retained cyberspace forces that operate CCMD networks and systems are assigned directly to various CCDR staffs. Certain Service-retained cyberspace forces are not SecDef-designated "cyberspace operations forces," including those whose primary purpose is to enable tactical C2 or the resiliency of weapons systems and CI/KR. In addition, the Defense Information Systems Agency (DISA) and various DOD agencies and activities employ civilian staff and contractors to perform these same operationalizing and DODIN operations functions. Other cyberspace forces may be established and staffed by the Services and the United States Special Operations Command when required to meet mission requirements. In addition, many CCMDs have organized their CO planning staff into a joint cyberspace center for unity of effort in planning, coordinating, integrating, synchronizing, and directing CCMD CO.

5. Challenges to the Joint Force's Use of Cyberspace

The JFC faces a unique set of persistent challenges executing CO and other operations in a constantly evolving, complex, and volatile global security environment characterized by contested norms of behavior in cyberspace and persistent disorder. To address these challenges, the JFC integrates CO with operations in all domains to support the DOD and CJCS global integration processes.

a. **Threats.** Cyberspace threats originate from states and their surrogates, criminal enterprises, individuals, and accidents and natural hazards, which together create a persistently contested environment in which the joint force plans and executes joint operations. USCYBERCOM follows a strategic approach of persistent engagement in cyberspace to preclude and defeat threats from malicious cyberspace activity (MCA).

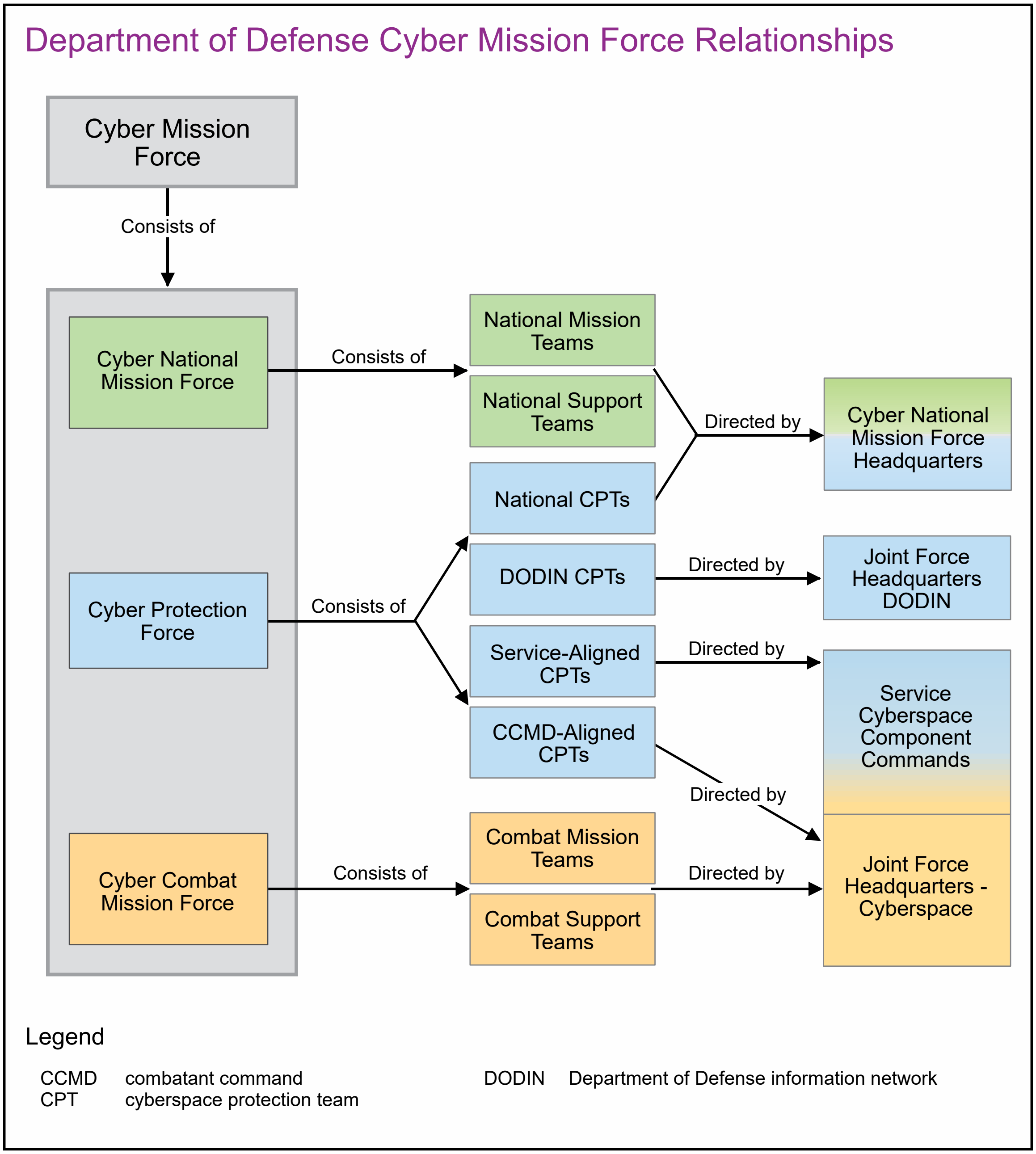

Department of Defense Cyber Mission Force Relationships
Cyber Mission Force
Consists of
Cyber National Mission Force
Consists of
National Mission Teams
National Support Teams
National CPTs
Directed by
Cyber National Mission Force Headquarters
Cyber Protection Force
Consists of
DODIN CPTs
Directed by
Joint Force Headquarters DODIN
Service-Aligned CPTs
Directed by
Service Cyberspace Component Commands
CCMD-Aligned CPTs
Directed by
Cyber Combat Mission Force
Consists of
Combat Mission Teams
Combat Support Teams
Directed by
Joint Force Headquarters - Cyberspace
Legend
CCMD combatant command
CPT cyberspace protection team
DODIN Department of Defense information network

Figure I-2. Department of Defense Cyber Mission Force Relationships

(1) **Nation-State Threat.** This threat is potentially the most dangerous because of nation-state access to resources, personnel, and time that may not be available to others. Some nations may employ cyberspace capabilities to gain strategic advantage over the United States. Nation-state threats involve adversaries; enemies; and potentially, in the case of espionage, even multinational partners. Nation-states may conduct operations directly or may outsource them to third parties, including front companies, patriotic hackers, or other surrogates, to achieve their objectives. Indirect or outsourced nation-state threat actors and their surrogates often operate in hidden or protected networks to mitigate risks to themselves and help confuse attribution.

(2) **Non-State Threats.** Non-state threats to the JFC's mission come from formal and informal organizations operating in cyberspace. These organizations are not bound by national borders and include nongovernmental organizations (NGOs), which may simply be working at cross-purposes to the joint force, and illegitimate organizations such as criminal organizations, violent extremist organizations, or other enemies and adversaries. Non-state threats use cyberspace to raise funds, communicate with target audiences and each other, recruit, plan operations, undermine confidence in governments, conduct espionage, and conduct cyberspace attacks. National or transnational criminal organizations steal information for their own use, including selling it to raise capital, and target financial institutions for fraud and theft of funds. Criminals often engage in cybercrime by targeting bank customers through fraud and business e-mail compromise rather than by stealing directly from banks. They also conduct cyberspace attacks using ransomware to acquire funds and may be part of a blended threat when they are used as surrogates by nation-states or non-state threats to conduct cyberspace attacks or espionage.

(3) **Individuals or Small-Group Threat.** Even individuals or small groups can threaten, attack, or exploit cyberspace, enabled by affordable and readily available techniques, technologies, and software or by authorized access in the case of insider threats. Their intentions are as varied as the number of groups and individuals involved. Ethical hackers may share vulnerability information with the DOD Vulnerability Disclosure Program, but, more frequently, these accesses are used with malicious intent. Some threats are politically motivated and use unauthorized access to spread their message. These small-scale threats can be co-opted by more sophisticated threats, such as criminal organizations or nation-states, often without their knowledge, to execute operations while concealing the identity of the threat/sponsor and creating plausible deniability.

(4) **Accidents and Natural Hazards.** The physical infrastructure of cyberspace is routinely disrupted by equipment failure, operator errors, industrial accidents, and natural disasters. These unpredictable events can have greater impact on joint operations than the actions of enemies. Recovery from accidents and hazardous incidents can be complicated by the requirement for significant coordination external to DOD and/or the temporary reliance on back-up systems or continuity of operations arrangements with which operators may not be proficient.

(5) **Anonymity and Difficulties with Attribution.** Attribution of threats in cyberspace is crucial to initiating a defensive response external to the protected cyberspace beyond that authorized as basic self-defense. The most challenging aspect of attributing actions in cyberspace is connecting a particular cyber-persona or action to a named individual, group, or nation-state with sufficient confidence and verifiability to hold them accountable. This effort requires significant analysis and, often, collaboration with non-cyberspace agencies or organizations. The nature of cyberspace, government policies, and laws, both domestic and international, present challenges to determining the exact origin of cyberspace threats. The ability to hide the sponsor and/or the threat behind a particular MCA makes it difficult to determine how, when, and where to respond. The anonymity of the Internet, combined with applications and technology intended to hide the identity of users, makes attribution a challenge for the foreseeable future. Effective information

sharing with intergovernmental, private-sector, and international partners can assist with the attribution challenge.

b. **Geographic Challenges.** Unlike the physical domains, cyberspace has no stateless maneuver space; it is all owned by someone. Therefore, when US military forces maneuver in gray and red cyberspace, mission and policy requirements may require clandestine maneuver, without the knowledge of the state where the infrastructure is located. Because CO can often be executed remotely, through a virtual presence enabled by wired or wireless access, many CO do not require physical proximity to the target but use remote actions to create effects. This represents an increase in operational reach not available in the physical domains. This use of global reach applies equally to both external missions in gray and red cyberspace, as well as internal missions in blue cyberspace. When remote access is not possible or preferable, cyberspace forces deploy to conduct expeditionary CO in the physical domains. The cumulative effects of some CO may extend beyond the initial target, a joint operations area (JOA), or outside of a single area of responsibility (AOR). Because of these transregional considerations, the requirement for global integration, and the need for high-demand forces and capabilities, some CO are coordinated, integrated, and synchronized using centralized execution from a location remote from the supported commander. Depending upon the geographic scope of the effect and amount of coordination required, CDRUSCYBERCOM may be a supported or supporting commander.

c. **Technology Challenges.** Using a cyberspace capability that relies on exploitation of technical vulnerabilities in the target may reveal its functionality and compromise the capability's effectiveness for future missions. This has implications for both external missions in gray and red cyberspace and internal missions in blue cyberspace. Cyberspace capabilities without hardware components can be replicated for little or no cost. This means, once discovered, these capabilities are widely available to adversaries and enemies, in some cases before protective measures in the DODIN can be updated to account for the new threat. In addition, since similar technologies share similar vulnerabilities, a single threat may be able to exploit multiple targets at once using the same malware or exploitation tactic. Computer programs such as malware can be modified (or designed to automatically self-modify), complicating efforts to detect and eradicate it. The IoT, artificial intelligence, quantum computing, and continued evolution of current technology (e.g., "6G" [sixth generation] mobile communications) and other developments will challenge and potentially disrupt the OE, requiring the joint force to remain agile and adaptable.

d. **Private Industry and Public Infrastructure.** Many of DOD's critical functions and operations rely on contracted commercial assets, including Internet service providers (ISPs) and global supply chains, over which DOD and its forces have no direct authority. This includes both data storage services and applications provided from a cloud computing architecture. Cloud computing enables DOD to consolidate infrastructure, leverage commodity IT functions, and eliminate functional redundancies while improving continuity of operations. However, the overall success of these initiatives depends upon well-executed risk mitigation and protection measures, defined and understood by both DOD components and industry. Dependency on commercial Internet providers means DOD coordination with the Department of Homeland Security (DHS), other interagency partners, and the private sector is essential to establish and maintain the security of DOD's information. DOD supports DHS, which leads interagency efforts to identify and mitigate cyberspace vulnerabilities in the nation's critical infrastructure. Sector risk management agencies, in coordination with DHS, assess sector risk, including identifying, assessing, and prioritizing risks, considering physical and cyberspace security threats, vulnerabilities, and consequences. DOD has the lead for improving security of the defense industrial base (DIB) sector, which includes major sector contractors and major contractor support to operations, regardless of corporate nation of domicile, and continues to support the development of whole-of-government approaches for DIB risk management. The global technology supply chain affects mission-critical aspects of the DOD enterprise, and the resulting IT risks can be effectively mitigated only through public-private-sector cooperation, such as the DOD's DIB Cybersecurity Program.

(1) **Globalization.** The combination of DOD's global operations with its reliance on cyberspace and associated technologies means DOD often procures mission-essential IT products and services from foreign vendors. A prime example is our reliance on network backbones and transmission equipment in other nations, such as undersea cables, fiber optic networks and telecommunications services, satellite and microwave antennas, and leased channels on foreign satellites. These systems may normally be reliable and trustworthy, but they can also leave US forces vulnerable to access denial by service interruption, communications interception and monitoring, or infiltration and data compromise. Another example is DOD's use of commercial, globally interconnected, globally sourced IT components in mission-critical systems and networks. Leveraging rapid technology development of the commercial marketplace remains a key advantage to DOD, but globally sourced technology provides adversaries the opportunity to compromise the supply chain to access or alter data and hardware, corrupt products, and intercept or deny communications and other mission-critical functions. Supply chain risks threaten all users and our collective security; therefore, DOD cannot ignore these risks to its missions. Globalization, including by US companies, introduces risks across the entire system lifecycle, to include design, manufacturing, production, distribution, operation and maintenance, and disposal of a system or component. Each of these lifecycle stages presents the opportunity to manipulate, deny, or collect information on such systems. It is not feasible to eliminate our reliance on foreign-owned services and products, but our reliance on them makes it essential that every reasonable avenue for risk mitigation be pursued, to include user and commander education at all levels, encryption, C2 system redundancy, operations security (OPSEC), and careful inspection of vendor-provided IT IAW DOD IT procurement policy.

(2) **Mitigations.** DOD partners with the DIB to increase the security of information about DOD programs residing on or transiting DIB unclassified networks. For example, in fiscal year 2020, DOD began implementing the DIB-focused Cybersecurity Maturity Model Certification framework. This framework provides a verification mechanism to ensure DIB partners have correctly implemented DOD cybersecurity policy to protect controlled unclassified information residing on their networks. The Department of Defense Cyber Crime Center (DC3) serves as DOD's operational focal point for the DIB Cybersecurity Program voluntary cyberspace threat information sharing, and mandatory

incident reporting, as required under the Defense Federal Acquisition Regulation Supplement. DC3 conducts analysis of DIB-reported threat information and offers analytical products that enable the DIB to better understand and defend against MCA. In addition, DOD is strengthening its acquisition regulations to require consideration of applicable cybersecurity policies during procurement of all DODIN components to reduce risks to joint operations.

Intentionally Blank

CHAPTER II
CYBERSPACE OPERATIONS CORE ACTIVITIES

> *"When I first started working cyberspace operations, these operations were often just concepts, and when conducted, performed ad hoc by technical specialists on loan from other organizations. Today this is not the case. Now, a mature and highly capable cyber force is built and in the fight, aggressively defending our network, conducting daily operations against adversaries, and strengthening the combat power and lethality of US forces around the world. This swift growth represents tremendous opportunity."*
>
> **Lieutenant General Paul Nakasone**
> **Prospective Commander, United States Cyber Command**
> **Testimony before Senate Committee on Armed Services**
> **March 1, 2018**

1. Introduction

a. CO are the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace. CO comprise the military, national intelligence, and ordinary business operations of DOD in and through cyberspace and are leveraged in support of each of the joint functions. Although commanders need awareness of the potential impact of the other types of DOD CO on their operations, the military component of CO is the only one guided by joint doctrine and is the focus of this publication. CCDRs and Services use CO to create effects in and through cyberspace. Military operations in cyberspace are organized into missions executed through a combination of specific actions. Various DOD agencies and components conduct national intelligence, ordinary business, and other activities in cyberspace. Although discussed briefly here for context, these activities are guided by DOD policies concerning CO but not by joint doctrine. While joint doctrine does apply to CSAs where it directly relates to their mission to support military forces, CSAs and other DOD agencies and activities primarily conduct various CO that are considered cyberspace-enabled activities.

b. **Cyberspace-Enabled Activities.** Most DOD uses of cyberspace enable other types of activities and employ cyberspace capabilities to complete tasks not undertaken as part of one of the three CO missions described below. These cyberspace-enabled activities include actions like operating a C2 or logistics system, commanding a satellite, sending an e-mail to support an information objective, using the Internet to complete an online training course, or developing a briefing. Other than being an authorized user of the network, DOD personnel need no special authorities to use cyberspace capabilities in this way. Also, it is through these routine uses of cyberspace that the majority of DODIN vulnerabilities are exposed to, and exploited by, our adversaries. The challenge is to train all DODIN users to understand the significance of cyberspace threats and to recognize threat tactics to minimize mission risk. Protecting the DODIN by establishing a culture of vulnerability awareness, particularly through DOD and interagency policies, practices, and training, is critical to the success of cyberspace-enabled DOD missions.

2. Military Operations In and Through Cyberspace

a. **Cyberspace Missions.** All actions in cyberspace that are not simply cyberspace-enabled activities are taken as part of one of three cyberspace missions: DODIN operations, defensive cyberspace operations (DCO), or offensive cyberspace operations (OCO). These three mission types, conducted under various sources of authority, comprehensively cover the activities of the cyberspace forces. The successful execution of CO requires integration, synchronization, and simultaneity of these missions. Military CO missions and their included actions are authorized by a military order (e.g., execute order [EXORD], operation order [OPORD], tasking order, verbal order), referred to hereafter as a mission order, issued under authority derived from law, regulations, directives, instructions, or policy. Cyberspace missions are categorized as DODIN operations, DCO, or OCO based only on the intent or objective of the issuing authority, not based on the cyberspace actions executed, the type of military authority used, the forces assigned to the mission, or the cyberspace capabilities employed. Some orders may cover multiple types of missions. For example, an internal mission standing order to protect the DODIN may include both DODIN operations and DCO mission components, and an order for an external mission in gray and red cyberspace could support both offensive and defensive objectives, based on the fundamental rationale for undertaking the mission. Defensive missions conducted in gray and red cyberspace are undertaken in self-defense against MCA, whereas offensive missions are power projection to create effects in cyberspace that support other military objectives.

b. Like missions in any other domain, completion of CO missions requires execution of specific actions, detailed in paragraph 2.c., "Cyberspace Actions." Effective execution of all cyberspace missions requires clear lines of C2; timely, relevant, and accurate intelligence and threat indicators from traditional and cyberspace sensors; vulnerability information from DOD and non-DOD sources; and accurate assessment of previous missions. IAW current USG policy, DOD deconflicts missions in gray and red cyberspace with the other USG department and agency mission partners who share this responsibility. Figure II-1 depicts a comprehensive framework of military CO, including the relationships between the cyberspace missions and actions. These mission and action descriptions are high-level. Therefore, although there are only three possible types of general CO missions, there can be various subordinate mission types under each of these three broad mission categories.

(1) **DODIN Operations.** The DODIN operations mission is to secure, configure, operate, extend, maintain, and sustain DOD cyberspace to create and preserve the confidentiality, availability, and integrity of the DODIN. This mission includes cyberspace security actions that address vulnerabilities of the DODIN or specific segments of the DODIN to prevent exploitation and operation of red teams and other forms of security evaluation and testing. DODIN operations also include a variety of cyberspace system operation actions like the set-up of tactical networks by expeditionary forces to extend existing networks, maintenance actions, and other non-security actions necessary for the sustainment of the DODIN. DODIN operations are network-focused and threat-agnostic: the cyberspace forces and workforce undertaking this mission endeavor to prevent all MCA

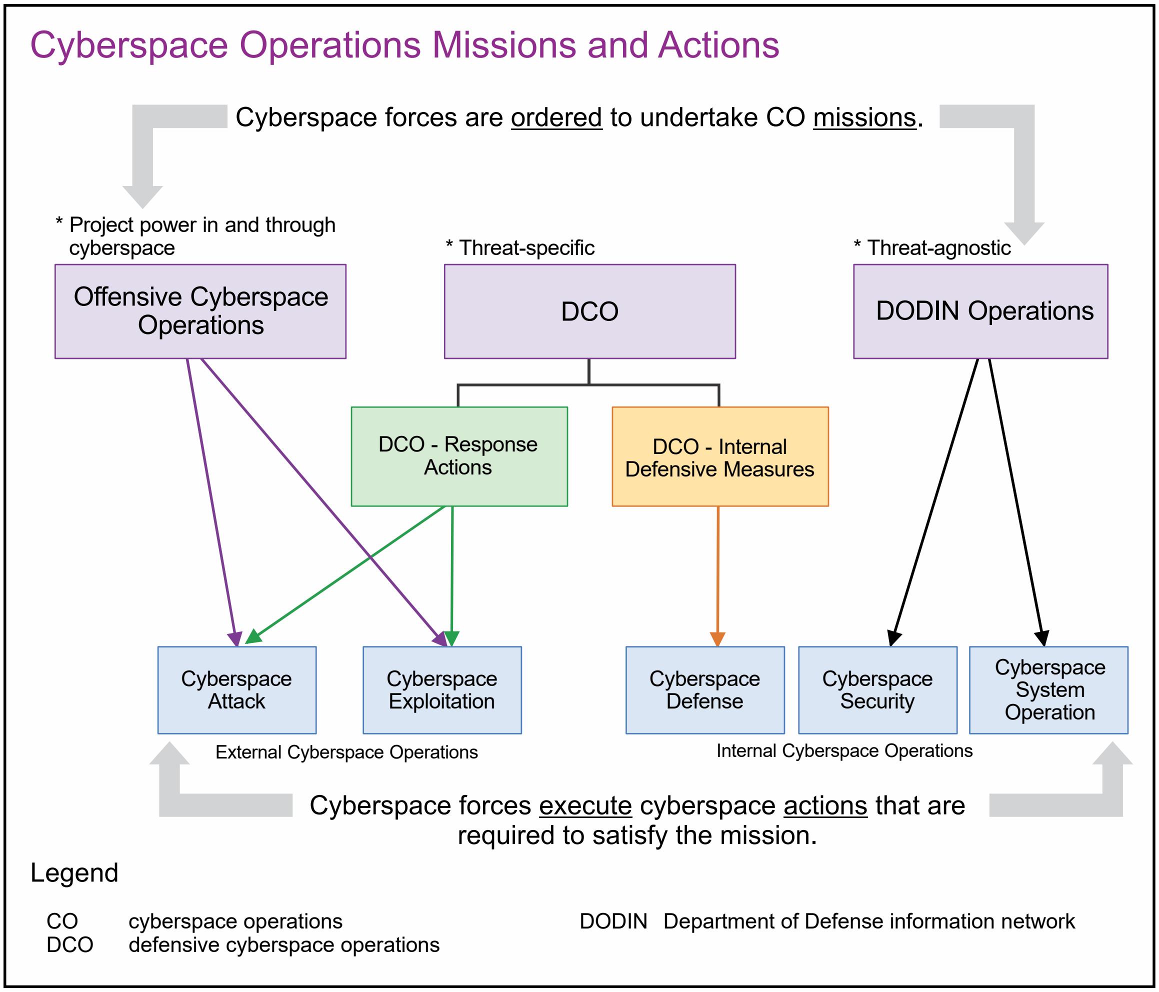

Cyberspace Operations Missions and Actions
Cyberspace forces are ordered to undertake CO missions.
* Project power in and through cyberspace
Offensive Cyberspace Operations
* Threat-specific
DCO
* Threat-agnostic
DODIN Operations
DCO - Response Actions
DCO - Internal Defensive Measures
Cyberspace Attack
Cyberspace Exploitation
Cyberspace Defense
Cyberspace Security
Cyberspace System Operation
External Cyberspace Operations
Internal Cyberspace Operations
Cyberspace forces execute cyberspace actions that are required to satisfy the mission.
Legend
CO cyberspace operations
DCO defensive cyberspace operations
DODIN Department of Defense information network

Figure II-1. Cyberspace Operations Missions and Actions

from negatively impacting a particular network or system they are assigned to secure. They are threat-informed and use all available intelligence about specific threats to improve the security posture of the network. DODIN operations are organized using the DODIN areas of operations and sectors established by USCYBERCOM and controlled by JFHQ-DODIN. DODIN operations do not include actions taken under statutory authority of a chief information officer (CIO) to provision cyberspace for operations, including IT architecture development; establishing standards; or designing, building, or otherwise operationalizing DODIN IT. DODIN operations is a standing mission, and although many DODIN operations activities are regularly scheduled events, they cannot be considered routine since their aggregate effect establishes the framework on which most DOD missions ultimately depend. The fundamental cyberspace action types of a DODIN operations mission are cyberspace security and cyberspace system operations.

See JP 6-0, Joint Communications System, *for a more detailed discussion of DODIN operations and the management of networked communication systems.*

(2) **DCO.** DCO missions are executed to defend blue cyberspace from imminent or active threats in cyberspace. Specifically, they are missions intended to preserve the

ability to utilize blue cyberspace capabilities and protect data, networks, cyberspace-enabled devices, and other designated systems by defeating ongoing or imminent MCA. This distinguishes DCO missions, which defeat specific threats that have bypassed, breached, or are threatening to breach security measures, from DODIN operations, which endeavor to secure DOD cyberspace from all threats in advance of any specific threat activity. DCO missions are conducted in response to specific threats of attack or exploitation and leverage information from maneuver, intelligence collection, counterintelligence (CI), LE, and other sources as required to enable mission assurance. DCO include countermeasures, outmaneuvering or interdicting adversaries taking or about to take actions against defended cyberspace, or otherwise responding to imminent internal and external cyberspace threats. The goal of DCO is to defeat the threat of a specific adversary and/or to return a compromised network to a secure and functional state. DCO protect cyberspace capabilities and services, including data, networks, cyberspace-enabled devices, PIT, and other designated systems. DCO include maneuver to gain or retain an advantageous position, including fires when authorized, against cyberspace threats emanating from outside the protected cyberspace. DCO halt a threat’s offensive initiative, sustain or regain friendly initiative, and, if required, create conditions for a counteroffensive. The two types of DCO are:

(a) **Defensive Cyberspace Operations-Internal Defensive Measures (DCO-IDM).** DCO-IDM are the form of DCO mission where authorized cyberspace defensive actions occur within the defended network or portion of cyberspace. DCO-IDM include risk- and intelligence-driven internal threat hunting for advanced and/or persistent threats, as well as the active internal countermeasures and responses to eliminate and mitigate these threats. CPT operations on MRT-C in response to indications of MCA, or before specific indicators of compromise exist, are an example of DCO-IDM. DCO-IDM also include active and passive internal countermeasures to defeat and mitigate the MCA. DCO-IDM of the DODIN is directed and synchronized by JFHQ-DODIN using a framework of DODIN areas of operations and sectors established by USCYBERCOM.

(b) **Defensive Cyberspace Operations-Response Actions (DCO-RA).** DCO-RA are the form of DCO mission where actions are taken external to the defended network or portion of cyberspace without the permission of the owner of the affected system. DCO-RA missions may rise to the level of use of force, with physical damage or destruction of enemy systems, depending on broader operational context, such as the existence or imminence of open hostilities, the degree of certainty in attribution of the threat, the damage the threat has caused or is expected to cause, and national policy considerations. DCO-RA missions, especially when they occur before an imminent threat has a chance to act, are defending forward in support of the persistent engagement strategic approach. As a self-defense mission, the authorizing official determines whether the exigence of the threat and other circumstances justify use of cyberspace exploitation and/or cyberspace attack.

(c) **DCO-IDM and DCO-RA in Defense of Non-DOD Cyberspace.** While DCO often focuses on protecting the DODIN, which includes all of DOD cyberspace, military cyberspace forces prepare to defend any US or other blue cyberspace when ordered. DOD operations rely on many non-DOD segments of cyberspace, including private-sector and mission-partner networks. Security of this cyberspace is the responsibility of the resource owners, which may include other USG departments and agencies, private-sector entities, and PNs. Since DOD-associated cyberspace is a known target for MCA, protection of these non-DOD networks and systems can be a vital component of mission assurance. If DCO-IDM missions are ordered as part of a defense support of civil authorities (DSCA) operation, Active Component units may support or be supported by National Guard (NG) forces activated under Title 32, United States Code (USC), if authorized by SecDef, or Title 10, USC; United States Coast Guard Forces under Title 14, USC; and/or other cyberspace forces from one of the Reserve Component (RC) units. CPTs defend forward when they deploy for expeditionary DCO-IDM missions to hunt for threats in gray or red cyberspace, at the invitation of a foreign government. These hunt forward operations (HFO) allow the United States to gain insight on MCA before it directly threatens US cyberspace.

(3) **OCO.** OCO are CO missions intended to project power in and through gray and red cyberspace through actions taken in support of CCDR or national objectives. OCO may exclusively target enemy cyberspace functions or create first-order effects in cyberspace to initiate carefully controlled cascading denial effects into the physical domains to affect weapon systems, C2 processes, logistics nodes, and other high-value targets. All CO missions conducted outside of blue cyberspace with a commander’s intent other than to defend blue cyberspace from an ongoing or imminent cyberspace threat are OCO missions. Depending upon the circumstances, OCO may be conducted under the same or similar external mission authorities as DCO-RA but are not directed at imminent threats in cyberspace, although OCO can include missions to defend against non-cyberspace threats. Like DCO-RA missions, some OCO missions may include cyberspace attack actions, including those that rise to the level of use of force, with physical damage or destruction of enemy systems. Specific effects created depend on the broader operational context, such as the existence or imminence of open hostilities and national policy considerations. All external missions require a properly coordinated military order and careful consideration of scope, rules of engagement (ROE), and measurable objectives. The fundamental cyberspace actions of an OCO mission are cyberspace exploitation and/or cyberspace attack.

c. **Cyberspace Actions.** Execution of any DODIN operations, DCO, or OCO mission requires completion of specific actions that employ cyberspace capabilities to create effects in cyberspace. All cyberspace mission objectives are achieved by the combination of one or more of five cyberspace actions, which are defined exclusively by the types of effects they create. As with the CO missions, the actions described below are only the primary categories of CO actions. CO planners and operators establish and use multiple subordinate activities under each of these five categories. The cyberspace actions are:

(1) **Cyberspace System Operation.** Cyberspace system operation actions are taken as part of the DODIN operations mission by communications and IT units and personnel to ensure specific segments of DOD cyberspace remain in operation to support user missions. These actions include non-security activities required for system administration, help desk functions, configuring and reconfiguring networks and system

components, management of telecommunications infrastructure, extending networks into new locations, and actions taken to meet periodic or emergent requirements for maintenance and repairs to cyberspace hardware components to maintain system availability. Cyberspace system operation actions comprise the bulk of the DODIN operations mission.

Note: Joint doctrine uses the term "cyberspace security" to distinguish this tactical-level cyberspace action from the policy and programmatic term "cybersecurity" used in the Department of Defense (DOD) and United States Government (USG) policy. To enable effective planning, execution, and assessment, doctrine distinguishes between cyberspace security and cyberspace defense actions, a distinction not made in DOD and USG cybersecurity policy, where the term cybersecurity includes the ideas of both security and defense. Doctrine uses "cyberspace security" to describe specific actions as described here and "cybersecurity" only in reference to DOD or national policies for protecting cyberspace.

(2) **Cyberspace Security.** Cyberspace security actions are part of the DODIN operations mission taken within protected cyberspace to reduce its vulnerability to MCA, including preventing unauthorized access to, exploitation of, or damage to computers; electronic communications systems; and other IT, including PIT, as well as the information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. Cyberspace security actions are risk-informed and network-focused, occurring in advance of a specific threat. Cyberspace security actions protect by reducing or eliminating vulnerabilities that may be exploited by a threat and/or by implementing measures to prevent MCA. Examples of cyberspace security actions include increasing password strength, enforcing two-factor authentication, installing a software patch to remove vulnerabilities, encrypting stored data, training users on cybersecurity policy best practices, restricting access to suspicious websites, and blocking traffic on unused router ports. Cyberspace security is enabled by, but does not include, physical security measures.

(3) **Cyberspace Defense.** Cyberspace defense actions are taken during DCO-IDM missions, within protected cyberspace, to discover and defeat specific threats that breach, threaten to breach, or are suspected to have breached the cyberspace security measures, to include actions that detect, characterize, fix, contain, clear, and recover/restore from MCA, including malware or the unauthorized activities of authorized users. The CCMD, Service, or DOD agency that provides or operates the network is generally authorized to take these defensive actions except in cases when they would negatively impact networks or systems outside the responsibility of the respective CCMD, Service, or agency. In some cases, CPTs are ordered to reinforce locally assigned forces for execution of cyberspace defense actions. JFHQ-DODIN directs and synchronizes all defensive actions that impact more than one CCMD or have impacts outside the responsibility of the network owner. Cyberspace defense actions are the only primary component action of DCO-IDM missions, although there are many subordinate types of defensive actions. Since both security and defense actions are crucial to safeguarding blue cyberspace, these actions are collectively referred to as protection.

(4) **Cyberspace Exploitation.** Cyberspace exploitation actions are a primary component of OCO and DCO-RA missions and include many types of subordinate actions in gray or red cyberspace that do not create cyberspace attack effects. Cyberspace exploitation actions include access creation, military intelligence activities, maneuver, information collection, and other enabling actions required to prepare for future military operations. Cyberspace exploitation includes actions to gain and maintain cyberspace superiority and support operational preparation of the environment for current and future operations through activities like gaining and maintaining unauthorized access to adversary networks, systems, and nodes of military value; maneuvering to positions of advantage; and positioning cyberspace capabilities to facilitate follow-on actions. Some of these cyberspace exploitation actions are considered **attack-specific preparations** if there is no possible explanation or purpose for them other than to enable a follow-on cyberspace attack. Cyberspace exploitation supports current and future operations through collection of information, including mapping red and gray cyberspace to support situational awareness; discovering vulnerabilities; enabling joint intelligence preparation of the environment, warning, and joint target development; and supporting the planning, execution, and assessment of military operations throughout the OE. Cyberspace exploitation actions are deconflicted with other USG departments and agencies IAW national policy.

(5) **Cyberspace Attack.** Cyberspace attack actions create noticeable denial effects (i.e., degradation, disruption, or destruction) in cyberspace or use manipulation in cyberspace that leads to denial effects in the physical domains. Cyberspace attack actions are a form of fires, taken when authorized as part of an OCO or DCO-RA mission. They are coordinated and deconflicted with other USG departments and agencies; are carefully synchronized with planned fires in the physical domains; and, except when specifically intended to result in physically destructive denial effects, do not rise to the level of armed attack or use of force under current international law. They include actions to:

(a) **Deny.** To prevent access to, operation of, or availability of a target function by a specified level for a specified time, to:

1. **Degrade.** To deny access to, or operation of, a target to a level represented as a percentage of capacity. Level of degradation is specified. If a specific time is required, it can be specified.

2. **Disrupt.** To completely but temporarily deny access to, or operation of, a target for a period of time. A desired start and stop time are normally specified. Disruption can be considered a special case of degradation where the degradation level is 100 percent.

3. **Destroy.** To completely and irreparably deny access to, or operation of, a target. Destruction maximizes the time and amount of denial. However, destruction is scoped according to the span of a conflict, since many targets, given enough time and resources, can be reconstituted.

(b) **Manipulate to Create Physical Effects.** This form of cyberspace attack controls or changes information, computers, information systems, and/or networks to create physical denial effects that may rise to the level of use of force or armed attack. Manipulation uses an enemy's information resources to create physical denial effects that may not at first appear to have been initiated from cyberspace, by employing deception, decoying, conditioning, spoofing (using forged identity), falsification, and other similar techniques against computer-controlled systems. The targeted computer system may seem to operate normally until secondary or tertiary physical effects reveal evidence of the logical first-order effect. See Chapter III, "Authorities, Roles, and Responsibilities," paragraph 4.b., "Application of the Law of War," for discussion of the legal considerations for using cyberspace attack capabilities that are intended to result in physical damage and/or lethal effects.

d. **Countermeasures in Cyberspace.** Countermeasures are that form of military science that, by the employment of devices and/or techniques, has as its objective the impairment of the operational effectiveness of enemy activity. In cyberspace, the term "countermeasures" applies to any CO actions that fit this description, regardless of where the action is taken. As in the physical domains, countermeasures in cyberspace can be taken either internal or external to the defended terrain and can be used preemptively or reactively. Internal countermeasures include cyberspace defense actions taken as part of a DCO-IDM mission; for example, closing router ports in use by an adversary for unauthorized access or blocking malware that is beaconing out of the DODIN. External countermeasures, which would be part of a DCO-RA or OCO mission, are employed beyond the boundary of blue cyberspace. In support of an OCO mission, they may be cyberspace attack actions that spoof or otherwise negate the effectiveness of adversary sensors or defenses. As part of a DCO-RA mission, they may be used to identify the source of a threat and/or use non-intrusive or minimally intrusive techniques to interdict or mitigate threats. External defensive countermeasures are normally nondestructive/nonlethal in nature; typically impact only the MCA but not the associated threat systems; and terminate when the threat stops. All external countermeasures are subject to the same synchronization, deconfliction, legal, and policy guidance as any other aspect of an OCO or DCO-RA mission.

e. **Assignment of Cyberspace Forces to CO.** Mission orders or other directives assign cyberspace forces described in Chapter I, "Overview of Cyberspace and Cyberspace Operations," to specific cyberspace missions.

(1) **Forces and Workforce Conducting Internal Missions.** Service-retained cyberspace forces, CCMD cyberspace forces, RC forces, and DOD agency and activity staffs execute much of the DODIN operations required to secure and operate the various backbones, sub-nets, segments, enclaves, and private networks of the DODIN, under the planning, direction, integration, and synchronization of the JFHQ-DODIN. These staffs include CSSPs established by the Services, CCMDs, and other DOD components to provide DODIN protection services under support agreements with system owners. Additionally, contracted personnel protect some segments of the DODIN. Given the complex, evolving, and federated nature of the DODIN, actions of system operators are

central to its protection. CPTs are a limited asset; therefore, the preponderance of responsibility for protection falls to CSSPs and system operators conducting DODIN operations and limited DCO-IDM as an integral part of their assigned duties. For example, operators of PIT have an implied responsibility to protect their equipment from cyberspace threats and require specialized training to detect and defeat these threats. Protecting PIT from MCA is complicated by the design of these systems, which are often developed with little consideration of cyberspace threats. Regardless of personnel and DODIN segments involved, when personnel with DODIN protection responsibilities detect compromise of cyberspace security measures, they transition, IAW standing authorities delegated by the commander, to the cyberspace defense actions of DCO-IDM to restore security to their assigned portion of the DODIN. Their effectiveness in making this transition depends upon their level of training and resources to detect and respond to threats. If discovery and mitigation of MCA requires expertise beyond that available to the network operator and/or the CSSP/ISP, CPTs may respond to provide supporting cyberspace defense actions, either remotely or by deploying to the affected location. Although network administrators and CSSPs do DCO-IDM when possible, as a first line of defense, CPTs are focused on DCO-IDM missions and provide significant additional cyberspace defense expertise. Like CMTs and NMTs, CPTs are military maneuver units that require robust intelligence support and coordinate and interoperate with the CO external mission forces to better understand threats. When necessary, CPTs perform other tasks to support network operators, including penetration testing, security surveys, and assessment. National-level CPT support is extended to defend non-DOD mission partner or critical infrastructure networks when ordered by SecDef, including DCO-IDM HFO as described previously.

(2) **Forces Conducting External Missions.** DCO-RA missions are normally assigned to NMTs, which are units of the CNMF that defend the DODIN or other blue cyberspace, when ordered. The NMTs are aligned under the CNMF-HQ against specific cyberspace threats. Although NMTs might conduct OCO against cyberspace threat targets, OCO missions are normally assigned to CMTs, tactical units of the CCMF that support CCDR plans and priorities to project power in support of national objectives. The CMTs are aligned, under the JFHQ-Cs, in support of CCMDs. In addition to NMTs and CMTs, the NSTs and CSTs provide specialized technical and analytic support for the units of the CMF. This support includes intelligence analysis, cyberspace capability development, linguist support, and planning. Although NMTs and CMTs generally train against different types of targets, the JFC is not restricted in their mission assignment, which is based on the best available unit or personnel, considering the mission objective.

f. **Referring to Cyberspace Capabilities.** Since capabilities are normally categorized by the types of effects they create, cyberspace capabilities are categorized by the cyberspace actions, not the cyberspace missions, which may have objectives that are too broad to be associated with a specific type of effect. Therefore, the most basic categories of cyberspace capabilities used on-net are: system operation, security, defense, exploitation, and attack. Below this level, capabilities are further divided into many categories and sub-categories. For example, one type of cyberspace exploitation capability creates access on a targeted system. Access capabilities may be further categorized into those that offer remote access or require close access or physical proximity; they may allow for wired or wireless access, and they may create persistent or only temporary access. In addition to cyberspace capabilities used to create objective effects on-net, other cyberspace capabilities fulfill enabling or service functions, like operating systems, launch platforms, mission training applications, or automated testing tools.

g. **Referring to Adversary Activities in Cyberspace.** The DOD CO mission labels of DODIN operations, DCO, and OCO are selected based on commander's objectives and intent and, therefore, may not accurately describe the actions of our adversaries and enemies in cyberspace, whose mission objectives and commander's intent are usually not known with certainty. Therefore, the term MCA refers generally to all adversary and enemy cyberspace threat activities. If the context of the discussion requires more specific descriptions of adversary activity, use terms descriptive of the specific effects (e.g., attack, exploitation, sabotage, access, maneuver) created by the MCA.

3. National Intelligence Operations In and Through Cyberspace

National-level intelligence organizations conduct intelligence activities in, through, and about cyberspace in response to national intelligence priorities. This intelligence supports military commanders' decision making and planning. Although DOD's cyberspace forces may collect tactically and operationally useful information while maneuvering to and through gray and red cyberspace, like all joint forces, they also depend on intelligence support from traditional military and national intelligence sources. National intelligence collection in and through cyberspace is not a military CO and is, therefore, a form of cyberspace-enabled activity.

See JP 2-0, Joint Intelligence, *for a more complete discussion of national intelligence activities, including intelligence federation. See Appendix A, "(U) Classified Planning Considerations for Joint Cyberspace Operations," for additional information about integration of military and national intelligence CO.*

4. Department of Defense Ordinary Business Operations In and Through Cyberspace

Ordinary business operations in and through cyberspace are cyberspace-enabled activities that comprise those non-intelligence and non-warfighting capabilities, functions, and actions used to support and sustain DOD forces and components. This includes the cyberspace-enabled functions of the many civilian-run DOD agencies and activities, such as the Defense Finance and Accounting Service and the Defense Contract Audit Agency. Since the conduct of DOD ordinary business operations in cyberspace is guided by DOD policy and not by joint doctrine, it is not discussed here in detail. However, vulnerabilities that may exist in the applications and devices used for DOD ordinary business operations might be exploited in a manner that directly impacts a military commander's mission. Since DOD agencies and activities use many of the same networks as military commanders, a compromise in any area of the DODIN used for business operations might result in a loss of mission assurance in cyberspace for military operations.

5. The Joint Functions and Cyberspace Operations

a. JP 3-0, *Joint Campaigns and Operations,* delineates the joint functions common to joint operations at all levels of warfare. These joint functions comprise related capabilities and activities grouped together to help commanders integrate, synchronize, and direct joint operations. This section presents an overview of how military operations leverage cyberspace capabilities to enable these functions in support of all DOD missions and how the functions themselves are accomplished in cyberspace during CO.

b. **C2.** Discussion of C2 and cyberspace requires a distinction between using IT systems that implement the C2 of all military operations and the C2 of forces that execute CO. The former, addressed here, is a cyberspace-enabled activity, and the latter is addressed in Chapter IV, "Planning, Coordination, Execution, and Assessment," paragraph 5, "Command and Control of Cyberspace Forces." C2 encompasses the exercise of authority and direction by commanders over assigned and attached forces in the accomplishment of their mission. Use of cyberspace as a means of exchanging communications is overwhelmingly the most common method at the strategic and operational levels of warfare and is increasingly important in tactical warfare. Digital communications methods have largely supplanted analog communications, except at the tactical level, where analog signaling will likely persist indefinitely for reasons of simplicity, reliability, and security. All military C2 systems that function by the transmission of digital data are part of the DODIN. Cyberspace provides communications pathways, planning and decision-support aids, and cyberspace-related intelligence to enable timely decision making and execution of those decisions. This provides the commander an advantage for controlling the timing and tempo of operations. Cyberspace offers an exceptionally diverse array of circuits for issuance of commands and signals to forces and for those forces to relay operational information back up the chain of command. Military orders converted to digital form, including digital voice and video, can travel on circuits that transit all of the physical domains, significantly increasing the likelihood of timely delivery. However, a commander's confidence in the C2 system can be easily compromised when the security of the DODIN becomes suspect; therefore, the more the commander relies on cyberspace for C2, the more important protection of these MRT-C assets is to this joint function.

See JP 3-30, Joint Air Operations; *JP 3-31,* Joint Land Operations; *JP 3-32,* Joint Maritime Operations; *and JP 3-14,* Joint Space Operations, *for more information on how cyberspace is used to enable operations in the physical domains.*

c. **Intelligence.** Understanding the OE is fundamental to all joint operations, including CO. Intelligence may be derived from information gained during military operations in cyberspace or from other sources. Intelligence operations in cyberspace not conducted by a military commander are covered in paragraph 3, "National Intelligence Operations In and Through Cyberspace," and Appendix A, "(U) Classified Planning Considerations for Joint Cyberspace Operations." All-source intelligence support to CO utilizes the same intelligence process used by all other military operations, with unique attributes necessary for support of CO planning detailed in Chapter IV, "Planning, Coordination, Execution, and Assessment." The process includes:

(1) Planning and direction, to include identification of target vulnerabilities to enable CI activities to protect against espionage, sabotage, and attacks against US citizens/facilities and continuously examining mission success criteria and associated metrics to assess the impact of CO and inform the commander's decisions.

(2) Tasking collection sensors with access to information about cyberspace.

(3) Processing and exploitation of collected data, including identification of useful information from collected data, either real-time or after-the-fact.

(4) Analysis of information and production of intelligence products.

(5) Dissemination and integration of intelligence related to cyberspace to the consumer.

(6) Evaluation and feedback regarding intelligence effectiveness and quality.

See JP 2-0, Joint Intelligence, *for more information on the joint intelligence process.*

d. **Fires.** Cyberspace attack capabilities create fires in and through cyberspace and are often employed with little or no associated physical destruction. However, modification or destruction of computers that control physical processes can lead to cascading effects (including collateral effects) in the physical domains. Depending upon the commander's objective, fires in cyberspace can be offensive or defensive, supporting or supported. Like all forms of fires, fires in and through cyberspace should be included in the joint planning and execution processes to facilitate synchronization and unity of effort and comply with the law of war and ROE. Fires in and through cyberspace encompass a number of tasks, actions, and processes, including joint targeting, coordination, and deconfliction. If multiple USG or allied entities have requirements to exploit or attack the same target in cyberspace, synchronization and deconfliction across all USG entities is required, otherwise their uncoordinated actions could expose or interfere with each other. Even if these effects can be created independently and are sufficiently justified, a technical analysis is still required to determine if the capabilities can operate as planned in the same environment without interference or increasing the chances of unwanted detection.

See JP 3-60, Joint Targeting, *for more information on joint targeting.*

e. **Movement and Maneuver**

(1) Movement and maneuver involves deploying forces and capabilities into an OA and positioning within that area to gain operational advantage in support of mission objectives, including accessing and, as necessary, controlling key terrain. Standardizing the organization and force structure of the units of the CMF and other cyberspace forces enhances their ability to maneuver in cyberspace, including deployment for expeditionary CO when necessary, although some CO can enable force projection without the need to

establish a physical presence in foreign territory. Maneuver in blue cyberspace includes employing forces, sensors, obstacles, threat hunting techniques, mitigation measures, and other cyberspace defense actions required to defeat active threats. Maneuver in gray and red cyberspace is a cyberspace exploitation action and includes such activities as gaining access to adversary, enemy, or intermediary links and nodes and shaping this cyberspace to support future actions. The ability to access or even control such terrain can change the outcome of an engagement. A significant factor in maneuverability in cyberspace is gaining and maintaining logical accesses within the OE. This capability to maneuver and provide operational reach may be lost at any time if the configuration of the relevant cyberspace is modified. The ubiquitous nature of cyberspace creates another major consideration because it enables an adversary or enemy to establish key points of presence outside the physical domains, in third-party nations and protected areas, or even inside the United States. Additionally, adversaries or enemies may conduct CO from physical network connections within the United States, PNs, or third-party nations, thereby limiting the JFC's maneuver options based on law and policy restriction and creating dependencies on our ability to coordinate with interagency and other mission partners to take action. Interagency and international partners have authorities and capabilities that can increase the costs incurred by adversaries by broadening the options available to the JFC against cyberspace threats and potentially reducing operational risk.

(2) Another component of maneuver in cyberspace is the ability to move data to a place or process where it has maximum military utility, including movement of data out of harm's way and into a secure location or process. Because of network latencies and performance differences between system messaging models, remote data stores are generally slower than local data stores. This could make the difference between success and failure in CO. In this context, having access to sufficient, secure, wired or wireless bandwidth is analogous to maintaining lines of communications in the physical domains. The ability to divert the flow of data from one physical link to another in the face of threats, for example from a terrestrial cable to a satellite communications (SATCOM) link or vice versa, is an example of freedom of maneuver in cyberspace. Therefore, managing the EMS within the OA is a key planning consideration for CO.

f. **Sustainment**

(1) Sustainment is the provision of logistics and personnel services to maintain operations through mission accomplishment and redeployment of the force. From the perspective of cyberspace-enabled activities in support of global logistics, DOD relies on protected DODIN and commercial network segments to coordinate sustainment of forces.

(2) Rapid advancements in IT require the development, fielding, and sustainment of cyberspace capabilities adaptable to the changing OE. For example, secure, wireless mobile devices provide anonymity for adversary Internet users; an adversary might update or change operating systems; or they may transition to using more secure virtual machines in their network architecture. Joint forces need the capability to adapt by rapidly incorporating new cyberspace capabilities into their arsenal. Additionally, the joint force may need the capability to quickly upgrade their own cyberspace capabilities to leverage

these same new technologies. However, pressure to deploy new technology should be balanced against the potential for increased risk and the requirements of cybersecurity policy, and implementation should be carefully orchestrated to prevent divergence among Service-provisioned cyberspace that could create vulnerabilities in DODIN architecture.

(3) Sustainment planning should identify and address legacy systems. Much of the legacy MRT-C was not designed and configured to be easily updated. As a result, many of the vulnerabilities on the DODIN are introduced via unpatched (and effectively un-patchable) systems. These vulnerabilities can be mitigated through additional layers of protection, which must be sustained to preserve mission assurance. Additionally, hardware capabilities, including sensors and other forward-deployed cyberspace capabilities, can deteriorate over time due to wear and tear or adversary discovery, requiring component repair or replacement to remain operable. This can be particularly problematic when physically inaccessible systems (such as those deployed to remote sites) require replacement or upgrade. It is vital commanders understand the mission risk created by leaving such cyberspace capabilities in place over long periods, not just to current operations but to the success of future DOD missions that rely on such capabilities. Finally, contingency software capabilities that are infrequently accessed may also require periodic refreshing and retesting to verify they are still secure and capable of creating the required effects, despite changes in the OE.

g. **Protection**

(1) Protection of the DODIN and other critical US cyberspace includes the continuous and synchronized integration of cyberspace security and, when required, cyberspace defense actions. Protection of cyberspace assets is complicated by their logical connectivity that can enable enemies to create multiple, cascading effects that may not be restricted by physical geography and civil/military boundaries. Cyberspace capabilities requiring protection include not only the infrastructure (computers, cables, antennas, and switching and routing equipment) but also parts of the EMS (datalink frequencies to include satellite downlink, cellular, and other wireless links) and the content (both data and applications) on which military operations rely. Key to DODIN protection is the positive control of all direct connections between the DODIN and public portions of cyberspace, as well as the ability to monitor, detect, and prevent the entrance of malicious network traffic and unauthorized exfiltration of information through these connections. Maintaining this control and the requisite blue cyberspace situational awareness is complicated by DOD’s acquisition of an increasing amount of technology, with access to the Internet (i.e., IoT), expanding the difficulty of mapping and monitoring the entire DODIN.

(2) Protection of blue cyberspace uses a combination of security and defensive cyberspace capabilities. Due to the speed of effects and the number of elements in cyberspace, automated procedures to defend cyberspace, verify configurations, and discover network vulnerabilities often provide a better chance of initial success against an aggressor than the manual equivalents. Several factors work against achieving perfect security of a collection of networks and systems as complex as the DODIN. Therefore, DODIN MRT-C is given priority for protection. Even the strongest encryption and most

secure protocols cannot protect the DODIN from poorly trained and/or unmotivated users who do not employ proper security practices. Therefore, the training of all DODIN users on appropriate behaviors and commanders' strict enforcement of cyberspace security best practices is part of an overall risk management program. Commanders are accountable for the actions of their personnel in cyberspace and should ensure clear understanding at all levels of the command of DOD cybersecurity policy standards and expectations.

(3) Protection of blue cyberspace is enhanced by a strategy of defending forward in gray and red cyberspace, including conducting DCO-IDM HFO with PNs, to get advanced warning of new threats. Protection of operational strengths, intent, timing, methods, and presence of cyberspace capabilities also requires strict adherence to unique OPSEC countermeasures, since some CO might be thwarted if these capabilities are discovered in advance of their effects. Concealment of movement within cyberspace uses different techniques than concealment in the physical domains. Skills such as avoiding detection are fundamental to most CO external missions and, therefore, essential to their protection.

(4) Force protection can be degraded by the way the joint force uses cyberspace. Modern tactical formations are highly digitized and increasingly connected through cyberspace and the EMS. The security of their use of cyberspace should be considered in force protection plans, since adversary and enemy MCA may result in increased risk to mission and risk to force if not mitigated.

For more information on OPSEC, refer to JP 3-13.3, Operations Security.

h. **Information**

(1) The information function encompasses the management and application of information and its deliberate integration with other joint functions to influence relevant actor perceptions, behavior, and/or action or inaction and to support human and automated decision making. The information function helps commanders and staffs understand and leverage the pervasive nature of information, its military uses, and its application during all military operations. This function provides JFCs the ability to integrate the generation, application, and preservation of friendly information while leveraging the inherent informational aspects of all military activities to achieve the commander's objectives and attain the end state. This joint force function supports actions that achieve objectives within the OEs and IEs. Since CO achieve objectives within cyberspace and cyberspace is wholly contained within the IE, it is important to understand its central relationship to the information joint function.

(2) The joint force conducts CO in concert with other operations, to gain and maintain an information advantage. Cyberspace is a domain through which specific information capabilities, such as MISO or MILDEC, may be employed. Note that while some OIE may be done using CO, they are still synchronized, integrated, and deconflicted with other activities and operations that impact the commander's objectives.

(3) It is important to understand that, although CO enable certain primary activities within the information function, there are information activities that do not involve CO. Therefore, failure to synchronize CO with other military operations' planning and execution can result in friendly forces conducting redundant or conflicting information activities, resulting in wasted time and resources and loss of operational advantage.

Refer to JP 3-04, Information in Joint Operations, *for information on the primary activities that support the information joint function.*

CHAPTER III
AUTHORITIES, ROLES, AND RESPONSIBILITIES

> *"I am counting on the leaders of our Department, the Military Departments and Services, the Joint Warfighting community, and our interagency partners to respond with vision and drive to this urgent call to action. We must prepare our Soldiers, Sailors, Airman, Marines, and DOD [Department of Defense] civilians with the personnel, capabilities, and authorities to defend our interests. Our way of life, and the future of our economic and military strength depend on it – we must succeed."*
>
> **James N. Mattis**
> **Secretary of Defense**
> ***The Department of Defense Cyber Strategy*, July 13, 2018**

1. Introduction

a. Under the authorities of SecDef, DOD uses cyberspace capabilities to shape cyberspace and provide integrated offensive and defensive options for the defense of the nation. USCYBERCOM coordinates with CCMDs, the JS, and the Office of the Secretary of Defense (OSD); liaises with other USG departments and agencies; and, in conjunction with DHS, DC3, and the Defense Counterintelligence and Security Agency, liaises with members of the DIB. Similarly, as directed, DOD deploys necessary resources to support efforts of other USG departments, as well as agencies and allies.

b. The *(U) National Military Strategy of the United States of America, 2022,* and *The Department of Defense Cyber Strategy* provide high-level requirements for national defense in cyberspace and DOD's role in defending DOD and larger US national security interests through CO.

c. **DOD's Roles and Initiatives in Cyberspace.** DOD's roles in cyberspace are, for the most part, the same as they are for the physical domains. As a part of its role to defend the nation from threats in cyberspace, DOD prepares to support DHS and the Department of Justice (DOJ), the USG leads for incident response activities during a national cybersecurity incident of significant consequences. To fulfill this mission, DOD conducts military operations to defend DOD elements of CI/KR and, when ordered, defends CI/KR related to vital US interests. DOD's national defense missions, when authorized by Presidential orders or standing authorities, take primacy over the standing missions of other departments or agencies. The *Department of Defense Cyber Strategy* establishes strategic initiatives that offer a roadmap for DOD to operate effectively in cyberspace, defend national interests, and achieve national security objectives.

d. **National Incident Response.** When directed, DOD provides cyberspace defense support during major cyberspace threat events to the United States. DOD coordinates with the requesting agency or department through the lead response department or agency, as described in the Presidential Policy Directive (PPD)-41, *United States Cyber Incident Coordination.* When civil authorities request such support, the fundamental principles of

DSCA used to respond to domestic emergencies in the physical domains also apply to defense support to cybersecurity incident response.

e. **CI/KR Protection.** CI/KR consist of the infrastructure and assets vital to the nation's security, governance, public health and safety, economy, and public confidence. IAW the *National Infrastructure Protection Plan,* DOD is designated as the sector risk management agency for the DIB. DOD provides cyberspace threat analysis and forensics support via the DIB Cybersecurity Program and the DC3. Concurrent with its national defense and incident response missions, DOD may be directed to support DHS and other USG departments and agencies to help ensure all sectors of cyberspace CI/KR are available to support national objectives. CI/KR protection relies on analysis, warning, information sharing, risk management, vulnerability identification and mitigation, and aid to national recovery efforts. Defense critical infrastructure (DCI) is a subset of CI/KR that includes DOD and non-DOD assets essential to project, support, and sustain military forces and operations worldwide. CCDRs with an assigned AOR have the responsibility to prevent the loss or degradation of DCI within their AORs and coordinate with the DOD asset owner, heads of DOD components, and defense infrastructure sector lead agents to fulfill this responsibility. CCDRs may act to prevent or mitigate the loss or degradation of non-DOD-owned DCI only in coordination with the CJCS and the Under Secretary of Defense for Policy and at the direction of SecDef IAW Department of Defense Directive (DODD) 3020.40, *Mission Assurance (MA).* As the lead agent of the DODIN sector of the DCI, the Commander, JFHQ-DODIN, is responsible for matters pertaining to the identification, prioritization, and remediation of critical DODIN infrastructure issues. Likewise, DOD coordinates and integrates, when necessary, with DHS for support of efforts to protect the DIB.

2. Authorities

a. Authority for CO actions undertaken by the Armed Forces of the United States is derived from the United States Constitution and federal law. Key laws that apply to DOD include Title 10, USC; Title 50, USC; and Title 32, USC. See Figure III-1 for a summary of applicable titles of USC as they apply to CO.

b. Authorities for specific types of military CO are established within SecDef policies, including DOD instructions, directives, and memoranda, as well as in EXORDs and OPORDs authorized by the President or SecDef and subordinate orders issued by commanders approved to execute the subject missions. These include the directive authority for cyberspace operations (DACO), established by CJCS EXORD, that enables CDRUSCYBERCOM's DOD-wide integrated and synchronized protection of the DODIN. The military missions and related actions of the cyberspace forces remain as described in Chapter II, "Cyberspace Operations Core Activities," regardless of the type of authority under which they are executed.

Refer to Appendix A, "(U) Classified Planning Considerations for Joint Cyberspace Operations," for additional information on authorities for CO.

Key Titles of United States Code Related to Cyberspace Operations

United States Code (USC)	Title	Key Focus	Principal Organization	Role in Cyberspace
Title 6	*Domestic Security*	Homeland security	Department of Homeland Security	Security of United States cyberspace
Title 10	*Armed Forces*	National defense	Department of Defense	Man, train, and equip United States forces for military operations in cyberspace.
Title 14	*Coast Guard*	Homeland security and law enforcement	Department of Homeland Security in peacetime, and Navy during wartime at direction of Congress	Crime prevention and apprehension of criminals operating in cyberspace.
Title 18	*Crimes and Criminal Procedure*	Law enforcement	Department of Justice	Crime prevention, apprehension, and prosecution of criminals operating in cyberspace.
Title 32	*National Guard*	National defense and civil support training and operations, in the United States	State Army National Guard, State Air National Guard	Domestic consequence management (if activated for federal service, the National Guard is integrated into the Title 10, USC)
Title 40	*Public Buildings, Property, and Works*	Chief Information Officer roles and responsibilities	All federal departments and agencies	Establish and enforce standards for acquisition and security of information technologies. Defines National Security Systems.
Title 44	*Public Printing and Documents*	Handling of public records	All Federal departments and agencies	Includes Federal Information Security Modernization Act, the Foundation of cybersecurity policy.
Title 50	*War and National Defense*	A broad spectrum of military, foreign intelligence, and counterintelligence activities	Commands, Services, and agencies under the Department of Defense and intelligence community agencies aligned under the Office of the Director of National Intelligence	Secure United States interests by conducting military and foreign intelligence operations in cyberspace. Establishes War Powers Resolution.

Figure III-1. Key Titles of United States Code Related to Cyberspace Operations

3. Roles and Responsibilities

a. **SecDef**

(1) Directs the military, intelligence, and ordinary business operations of DOD in cyberspace.

(2) Provides policy and guidance for employment of forces conducting CO missions through the Under Secretary of Defense for Policy, SecDef's Principal Cyber Advisor, and the Deputy Assistant Secretary of Defense for Cyber Policy.

(3) Develops and issues the *DOD Information Resources Management Strategic Plan* through the DOD CIO. The DOD CIO is the DODIN architect and, as such, develops, maintains, and enforces compliance with DODIN architecture standards and cybersecurity policy. Inherent in the DOD CIO's architecture responsibility are the responsibilities for interoperability, data sharing, effective use of enterprise services, EMS management, and DODIN program synchronization.

(4) Develops and oversees implementation of DOD policy, strategy, programs, and guidance regarding: intelligence; CI; security; sensitive activities; and other intelligence-related matters in cyberspace, to include all intelligence, surveillance, and reconnaissance (ISR) activities and associated tasking, processing, exploitation, and dissemination through the Under Secretary of Defense for Intelligence and Security IAW DODD 5143.01, *Under Secretary of Defense for Intelligence and Security (USD[I&S]).*

(5) Coordinates with Secretaries of other USG departments to establish appropriate representation and participation of personnel on joint interagency coordination groups (JIACGs), working groups, task forces, and collaboration and deconfliction bodies.

b. **The CJCS**

(1) Advises the President and SecDef on operational policies, responsibilities, and programs, including the global integration of military operations.

(2) Assists SecDef in implementing operational responses to threats in cyberspace.

(3) Translates SecDef guidance into orders and CJCS issuances as required.

(4) Ensures cyberspace plans and operations are compatible with other military plans and operations.

(5) Assists CCDRs in meeting SecDef-approved operational requirements.

c. **Service Chiefs**

(1) Provide appropriate administration of and support to cyberspace forces, including units of the CMF, Service-retained forces, and forces assigned or attached to CCMDs.

(2) Train and equip cyberspace forces and develop cyberspace capabilities for deployment/support to CCMDs, as directed by SecDef.

(3) Comply with CDRUSCYBERCOM's direction for security, operation, and defense of their respective Service segments of the DODIN, including applicable direction issued under CDRUSCYBERCOM's DACO, either from USCYBERCOM directly or from JFHQ-DODIN or the SCCs, as delegated.

(4) Coordinate with CDRUSCYBERCOM to prioritize CO mission requirements and force capabilities.

(5) Provide users of the EMS with regulatory and operational guidance in the use of frequencies through the authority of Army (Army Spectrum Management Office), Navy (Navy and Marine Corps Spectrum Center), and Air Force (Air Force Spectrum Management Office).

d. **Chief, National Guard Bureau**

(1) Advises the CJCS and CDRUSCYBERCOM on NG matters pertaining to CCMD CO missions, and supports planning and coordination for such activities as requested by the CJCS or the CCDRs.

(2) Serves as the channel of communications on all CO matters pertaining to the NG between USCYBERCOM and the 50 states, the Commonwealth of Puerto Rico, the District of Columbia, Guam, and the United States Virgin Islands.

(3) Responds to direction from USCYBERCOM and JFHQ-DODIN, issued under DACO, to secure, operate, and defend the NG segments of the DODIN.

e. **CDRUSCYBERCOM**

(1) Plans and executes global CO as directed. As the coordinating authority for planning CO, coordinates, integrates, synchronizes, deconflicts, and conducts activities to:

(a) Direct the security, operations, and defense of the DODIN.

(b) Prepare to, and when directed, conduct military CO in gray and red cyberspace, in support of national objectives.

(c) Provide situational awareness, warning, assessment, and defense against significant foreign cyberspace threats to the United States and its interests.

(d) Advocate for cyberspace capabilities.

(2) Exercises COCOM of the CMF and other cyberspace forces as assigned.

(3) Deconflicts cyberspace exploitation and cyberspace attack actions IAW national and DOD policy. Deconflicts influence operations within cyberspace.

(4) As directed by SecDef, serves as the supported commander for CO in coordination with affected CCDRs. If the scope of the CO spans multiple CCMD AORs, CDRUSCYBERCOM is the supported commander. For theater-specific events, CDRUSCYBERCOM may be designated a supporting or supported commander, depending upon the order issued. CCDRs are supported or supporting, as appropriate, for theater/functional DODIN operations and DCO-IDM.

(5) Leverages IC sensors and directs DODIN sensors, as appropriate, to establish and share comprehensive situational awareness of red, gray, and blue cyberspace in support of assigned missions and CCDRs requirements.

(6) Coordinates with the IC, CCMDs, Services, DOD agencies and activities, and multinational partners to facilitate development of improved access to gray and red cyberspace to support planning and operations.

(7) As directed, provides military representation to USG departments and agencies, US commercial entities, and international organizations for cyberspace matters.

(8) Notifies the CCMDs of ongoing or developing cyberspace threats and anomalies to reduce potential risks and effectively integrate systems, networks, services, and EMS usage and to ensure compliance with DOD-mandated DODIN configuration standards.

(9) Performs analysis of threats to the DODIN, including threat analysis of MCA. In coordination with CCMDs, changes the global protection posture of the DODIN, as warranted by threat assessments. Serves as supported commander for DCO-IDM response to global cybersecurity threat events.

(10) Plans for and, as directed, coordinates or executes DCO to defend US CI/KR and other blue cyberspace.

(11) In coordination with CCMDs, annually recommends cyberspace force mission alignment, through the JS, to SecDef for approval.

(12) As joint force provider for CO, identifies and recommends global joint sourcing solutions to the CJCS, in coordination with the Services and other CCMDs, and supervises implementation of sourcing decisions.

(13) As joint force trainer for SecDef-designated "cyberspace operations forces:"

(a) Establishes and maintains training and certification standards.

(b) Develops instructions and orders for provisioning and training.

(c) Conducts and supports CO in joint training exercises.

(14) Develops recommendations to the CJCS regarding strategy, policy, doctrine, tactics, techniques, and procedures for CO and the joint employment of cyberspace forces.

(15) Plans, conducts, and provides oversight of cybersecurity policy inspections IAW Department of Defense Instruction (DODI) 8530.01, *Cybersecurity Activities Support to DOD Information Network Operations,* and conducts public key infrastructure audits IAW DODI 8520.02, *Public Key Infrastructure (PKI) and Public Key (PK) Enabling.*

(16) Is dual-hatted as the Director, National Security Agency/Central Security Service.

(17) **Supporting Commanders and Elements**

(a) **Commander, JFHQ-DODIN.** In coordination with all CCDRs and other DOD components, conducts the operational-level planning, direction, integration, synchronization, and execution of DODIN operations and DCO-IDM missions to defend the DODIN. Maintains support relationships, as established by CDRUSCYBERCOM, with all CCDRs for theater/functional DODIN operations and DCO-IDM. Commander, JFHQ-DODIN, is supported for global DODIN operations and DCO-IDM, and CCDRs are supported for DODIN operations and DCO-IDM with effects contained within their assigned AOR or functional mission area. Exercises DACO over all DOD components as delegated by CDRUSCYBERCOM, using DODIN areas of operations and sectors to organize cyberspace security and cyberspace defense actions. Exercises OPCON of assigned CPTs.

(b) **Commander, CNMF-HQ.** When directed, conducts the defense of the nation's cyberspace through operational-level planning, coordination, execution, and oversight of DCO-RA missions and employment of national CPTs on DCO-IDM missions focused on threats to critical blue cyberspace outside the DODIN. Exercises OPCON of assigned NMTs, NSTs, and CPTs.

(c) **Commanders, SCCs.** Execute Service component functions in support of USCYBERCOM. In coordination with Commander, JFHQ-DODIN, conduct the operational-level planning, direction, coordination, execution, and oversight of DODIN operations and DCO-IDM within their Service segments of the DODIN. To achieve unity of action for protection of the DODIN, as directed, exercise DACO over organizations within their Service that take cyberspace security and cyberspace defense actions across assigned DODIN areas of operations. Exercise administrative control of Service cyberspace forces, to include those that are presented by the Services and assigned to CDRUSCYBERCOM as reflected in the *Forces for Unified Commands Memorandum ("Forces For") Assignment Tables* IAW the GFMIG. Exercise OPCON of Service CPTs.

(d) **Commanders, JFHQ-C.** Analyze, plan, and execute CO missions in general support of the CCDRs. Focus on supporting commander's critical information requirements, providing expertise regarding feasibility of courses of action, and integrating CO into CCDR plans and orders. Exercise OPCON of assigned CPTs, CMTs, and CSTs.

(e) **USCYBERCOM Cyberspace Operations-Integrated Planning Elements (CO-IPEs).** Integrate within a CCDR's CO planning staff to provide direct support CO expertise and reachback capability to USCYBERCOM. CO-IPEs, under the supervision of their CCMD-associated joint force headquarters (JFHQ), have direct liaison authorized to all USCYBERCOM components to support the CCDR. CO-IPEs are staffed by the SCCs and are co-located with each CCMD for full integration into their staffs, as determined by the CCDR. They are forward extensions of the JFHQ-C that supports their CCMD and of JFHQ-DODIN, except for the United States Transportation Command CO-IPE, which is solely an extension of the JFHQ-DODIN. CO-IPEs provide a CCDR with CO planners and other subject matter experts required to support development of CCMD requirements for CO and to assist CCMD planners with coordinating, integrating, and deconflicting CO.

f. **Other CCDRs**

(1) Secure, operate, and defend tactical and constructed DODIN segments within their commands and AORs.

(2) Integrate CO into plans (e.g., CCMD campaign plans, concept plans, and operation plans); integrate cyberspace capabilities into military operations as required; and work closely with the joint force, USCYBERCOM, SCCs, and DOD agencies to create fully integrated capabilities.

(3) In coordination with USCYBERCOM, as required through their respective JFHQ-C and CO-IPE, orchestrate planning efforts for CO, designate the desired effects of CO, and determine the timing and tempo for CO conducted in support of their missions. CCDRs with functional responsibilities direct DODIN operations and DCO-IDM over DODIN segments under their control, consistent with those responsibilities.

(4) CCDRs with an assigned AOR prioritize and request theater-specific DCO-IDM in response to compromises of DODIN security in coordination with JFHQ-DODIN, through the unified command theater network control center or equivalent organization. For cybersecurity events that have been categorized as a global event by USCYBERCOM, CDRUSCYBERCOM is the supported commander for the DCO-IDM, and other CCDRs support response efforts and tasking from JFHQ-DODIN.

(5) Serve as a focal point for in-theater DODIN operations that integrate multinational partners.

(6) Plan for communications system support of operations that may be directed by SecDef and ensure the interoperability of DOD forces with non-DOD mission partners in terms of equipment, procedures, and standards.

(7) Retain authority to approve or deny DOD component-initiated modifications to the DODIN that impact in-theater operations only.

(8) In coordination with the DOD asset owner, heads of DOD components, and DOD infrastructure sector lead agents, CCDRs with an assigned AOR act to prevent the loss, degradation, or other denial of DOD-owned DCI within their AORs. Act only in coordination with the CJCS and Under Secretary of Defense for Policy to prevent or mitigate the loss or degradation for non-DOD-owned DCI.

(9) In coordination with CDRUSCYBERCOM, advocate for cyberspace capabilities and resources needed to support the CCDR's missions.

(10) Provide users of the EMS with regulatory and operational guidance in the use of required frequencies for CO IAW coordinated agreements between US forces and PNs.

(11) In coordination with CDRUSCYBERCOM, conduct CO within assigned AORs.

(12) In coordination with CDRUSCYBERCOM, ensure CO security cooperation activities and cyberspace capability development actions support DOD priorities, goals, and objectives and are consistent with USCYBERCOM and CCDR responsibilities.

g. **Commanders, United States Indo-Pacific Command and United States Northern Command.** In addition to responsibilities in paragraph 3.f., "Other CCDRs," these CCDRs fulfill specific CO responsibilities related to DSCA and homeland defense in coordination with CDRUSCYBERCOM.

h. **Commander, United States Space Command (CDRUSSPACECOM).** In addition to responsibilities in paragraph 3.f., "Other CCDRs," CDRUSSPACECOM fulfills specific CO-related SATCOM responsibilities.

(1) Represents the DOD SATCOM community by coordinating consolidated user positions with CCMDs, Services, DOD agencies, and international partners. CDRUSSPACECOM has operational and configuration management authority for the SATCOM component of the DODIN in all three segments of space operations (orbital, link, and terrestrial). Directs day-to-day operations of DOD-owned and leased SATCOM resources. Coordinates international partner and non-DOD SATCOM resources used by DOD to support mission requirements.

(2) Develops, coordinates, and executes SATCOM operations policies and procedures; constellation deployment plans; and satellite positioning, repositioning, and disposal plans. Assesses, in collaboration with DISA and JFHQ-DODIN, how these various plans impact communications support to current and future operations, operation plans, and concept plans. Except in the case of emergencies, CDRUSSPACECOM coordinates SATCOM actions with users prior to execution.

i. **Commander, United States Special Operations Command.** In addition to responsibilities in paragraph 3.f., "Other CCDRs," Commander, United States Special Operations Command, organizes, trains, and equips special operations forces to conduct CO and plans and executes CO as authorized.

j. **Commander, United States Strategic Command.** In addition to responsibilities in paragraph 3.f., "Other CCDRs," Commander, United States Strategic Command, fulfills specific responsibilities related to the nuclear command, control, and communications (NC3) portion of the DODIN. As the NC3 enterprise lead, Commander, United States Strategic Command, oversees and manages NC3 enterprise operations, requirements, and systems engineering and integration functions. This includes, in coordination with JFHQ-DODIN, direction of cyberspace security and cyberspace defense actions across all NC3 systems and platforms.

k. **Director, DISA**

(1) Complies with CDRUSCYBERCOM direction, issued by the commander of JFHQ-DODIN under delegated DACO, to execute DODIN operations and DCO-IDM missions at the global and enterprise level within DISA-operated portions of the DODIN.

(2) Provides engineering, architecture, and provisioning support for integrated DODIN operations, including enterprise management, content management, and mission assurance, including terrestrial communications infrastructure, undersea cables, and associated landing sites.

(3) Provides shared situational awareness of DISA-operated portions of the DODIN.

(4) Supports CDRUSSPACECOM by acquiring commercial SATCOM and DOD gateways. Establishes security requirements in the development of DISA security technical implementation guides for IT that provide unified capabilities over the SATCOM segment of the DODIN and verifies compliance during assessments or inspections.

(5) Mitigates SATCOM service outages and plans and executes service restoration at the global and enterprise level, as directed by commander of JFHQ-DODIN.

(6) Provides and maintains a critical nodes defense plan for long-haul communications.

(7) Is dual-hatted as the Commander, JFHQ-DODIN.

l. **Director, National Security Agency/Chief, Central Security Service**

(1) Provides signals intelligence (SIGINT) to national policy makers and military forces; cybersecurity policy guidance and assistance to DOD components, DIB, and national customers; and technical support, including encryption and cross-domain network

solutions, pursuant to DOD policy (DODI 8500.01, *Cybersecurity;* DODI 8530.01, *Cybersecurity Activities Support to DOD Information Network Operations;* DODI 8560.01, *Communications Security [COMSEC] Monitoring;* DODD 5100.20, *National Security Agency/Central Security Service [NSA/CSS]);* Executive Order 12333, *US Intelligence Activities,* as amended; Executive Order 14028, *Improving the Nation's Cybersecurity*; National Security Memorandum-8, *Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems;* and National Security Directive 42, *National Policy for the Security of National Security Telecommunications and Information Systems.*

(2) Provides DOD with capacity/capability in both cyberspace security and cyberspace defense products and expertise and intelligence support required to execute CO, including operation of cyberspace perimeter defenses under direction of USCYBERCOM; target development assistance; situational awareness and attack sensing and warning; threat analysis; internal threat hunting; red-teaming and security assist visits; communications monitoring; forensics; linguist support; and other specialized support, as authorized.

Refer to Appendix A, "(U) Classified Planning Considerations for Joint Cyberspace Operations," for additional information on National Security Agency support to military CO.

m. **Director, Defense Intelligence Agency (DIA)**

(1) Provides timely, objective, and relevant military intelligence to warfighters, defense planners, and defense and national security policy makers.

(2) Conducts all-source analysis in support of CO, to include dynamic threat assessments and campaign intelligence estimates that contribute to CCMD development of CO-related joint intelligence preparation of the OE products.

(3) Serves as the DOD focal point for all CI in cyberspace investigations and operations. In conjunction with the Military Departments and DOD agencies, DIA strives to identify and neutralize all CI-related cyberspace threats to DOD. DIA supports CI operations in cyberspace to promote cyberspace superiority and provides worldwide cyberspace CI situational awareness and coordination.

(4) In coordination with the JS, Services, other DOD agencies and activities, OSD, engineers, develops, implements, and manages the sensitive compartmented information portion of the DODIN, including the configuration of information, data, and communications standards for intelligence systems. Included within this is the overall responsibility for the operation of the Joint Worldwide Intelligence Communications System, a strategic, secure, high-capacity telecommunications network serving the IC with voice, data, and video services. DIA establishes defense-wide intelligence priorities for achieving interoperability between tactical, theater, and national intelligence-related systems and between intelligence-related systems and the tactical, theater, and national elements of the DODIN.

(5) Sets policies, standards, and requirements for joint targets, including the virtual elements of facility, individual, organization, and equipment targets. All joint target development, to include targets in support of CO, adheres to the standards put forth in Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3370.01, *Target Development Standards.*

n. **Director, DC3.** Administratively assigned to the Department of the Air Force but supporting the entire DOD, the DC3:

(1) Provides digital and multimedia forensics; cybersecurity incident investigative and technical training; technical solutions research, development, test, and evaluation; critical infrastructure protection; and cyberspace vulnerability analysis for DODIN protection, LE, IC, CI, and counterterrorism organizations.

(2) Serves as the DOD center of excellence and establishes DOD standards for digital and multimedia forensics.

(3) Serves as the operational focal point for the DIB cyberspace threat information sharing activities performed to protect unclassified DOD information that transits or resides on unclassified DIB information systems and networks.

(4) Administers the DOD Vulnerability Disclosure Program, managing the assessment, submission, and remediation of vulnerabilities identified in all publicly accessible DOD information systems.

o. **Other DOD Agencies and Activities.** All DOD agencies and activities are responsible for developing, maintaining, and operating their IT in a manner consistent with and reflective of applicable DODIN architecture and cybersecurity policy standards, and they plan, resource, acquire, implement, and maintain agency-specific IT IAW DOD policy and resource priorities. DOD agencies that are also part of the IC are additionally subject to the policies and guidance of the IC CIO. All DOD agencies and activities respond to direction from USCYBERCOM and JFHQ-DODIN, issued under DACO, to secure, operate, and defend their segments of the DODIN.

p. **DHS**

(1) Secures US cyberspace, at the national level, by protecting non-DOD USG networks against cyberspace exploitation and attacks, including actions to reduce and consolidate external access points, deploy passive network defenses and sensors, and define public and private partnerships in support of national cybersecurity policy.

(2) Protects USG network systems from cyberspace threats and partners with government, industry, and academia, as well as the international community, to make cybersecurity a national priority and a shared responsibility.

(3) Pursuant to the Homeland Security Act of 2002 and Homeland Security Presidential Directive-5, *Management of Domestic Incidents,* the Secretary of Homeland Security is the principal federal official for domestic incident management. Pursuant to PPD-41, *United States Cyber Incident Coordination,* DHS is the lead federal agency for cybersecurity incident asset response. When an incident affects a private entity, the relevant sector risk management agency will generally coordinate the USG's efforts to understand the potential impact on private-sector critical infrastructure, including within the DIB. For significant cybersecurity incidents external to the DODIN and IC networks, DHS's Cybersecurity and Infrastructure Security Agency is the lead federal agency for technical assistance and vulnerability mitigation.

(4) Partners with USCYBERCOM, the IC, DOJ, and other LE and CI agencies for identification and sharing of MCA indications and threat warning.

q. **DOJ**

(1) DOJ, including the Federal Bureau of Investigation (FBI), leads counterterrorism and CI investigations and related LE activities associated with government and commercial CI/KR. DOJ investigates, defeats, prosecutes, and otherwise reduces foreign intelligence, terrorist, and other cyberspace threats to the nation's CI/KR. The FBI is the lead agency for significant cybersecurity incident investigation activities, except those that affect the DODIN or the IC. Given the ability of MCA to spread, investigation of serious cybersecurity threats to the DODIN are coordinated with the FBI.

(2) The FBI also conducts domestic collection, analysis, and dissemination of cybersecurity threat information and operates the National Cyber Investigative Joint Task Force, a multiagency focal point for coordinating, integrating, and sharing pertinent information related to cybersecurity threat investigations, with representation from DHS, the IC, DOD, and other agencies as appropriate.

4. Legal Considerations

a. DOD conducts CO in compliance with US domestic law, applicable international law, and relevant USG and DOD policies. Laws applicable to military activities in the United States also apply to cyberspace. DOD cyberspace forces generally operate either on the DODIN or, when properly authorized, in gray and red cyberspace, or other blue cyberspace, when, for example, conducting HFO or DSCA under appropriate authority. Each CO mission has unique legal considerations. Before conducting CO, commanders, planners, and operators require clear understanding of the relevant legal framework to ensure compliance with laws and policies. It is essential that commanders, planners, and operators consult with legal counsel during planning and execution of CO.

b. **Application of the Law of War.** Members of DOD comply with the law of war during all armed conflicts, however characterized. In all other military operations, members of DOD act consistent with the law of war's fundamental principles and rules, which include those in Common Article 3 of the 1949 Geneva Conventions and the principles of military necessity, humanity, distinction, proportionality, and honor. The law of war consists of the treaties and customary international law binding on the United States that regulate the resort to armed force; the conduct of hostilities and the protection of war victims in international and non-international armed conflict; belligerent occupation; and the relationships between belligerent, neutral, and nonbelligerent states. The law of war rests on fundamental principles of military necessity, humanity, proportionality, distinction (discrimination), and honor. Precisely how the law of war applies to CO is not fully settled, and some aspects of the law in this area will continue to develop, especially as new types of cyberspace capabilities emerge and nations determine their views in response to such developments. Specific law of war rules may apply to CO, even though those rules were developed before CO were conceived. Applicability of specific rules depends upon whether a proposed operation constitutes an armed attack or use of force under international law. Therefore, use of cyberspace attack capabilities that are intended to manipulate physical systems to create destructive or lethal effects is subject to the same procedural and legal review as the use of traditional lethal weapons. Likewise, CO that do not constitute an armed attack under international law are not strictly bound by the international law principles applicable to such attacks. When no specific law of war rule or other applicable rule applies, law of war principles provide a general guide for conduct during CO. Use of the terms “cyberspace attack capability” or even “cyberspace weapon” are means to identify requirements and to support resource allocation for warfighting in cyberspace and are not determinant as to whether a resource or capability is a weapon or weapon system IAW international law; Title 10, USC, Section 396; DOD issuances; joint doctrine; or Service regulations.

See JP 3-84, Legal Support; *DODD 2311.01,* DOD Law of War Program; *CJCSI 5810.01,* Implementation of the DOD Law of War Program; *and the* Department of Defense Law of War Manual *for more information on the law of war.*

CHAPTER IV
PLANNING, COORDINATION, EXECUTION, AND ASSESSMENT

> *"We're trying to both physically and virtually isolate ISIL [Islamic State of Iraq and the Levant], limit their ability to conduct command and control, limit their ability to communicate with each other, limit their ability to conduct operations locally and tactically. I'll be one of the first ones arguing that that's about all we should talk about. We want them to be surprised when we conduct cyber[space] operations. And, frankly, they're going to experience some friction that's associated with us and some friction that's just associated with the normal course of events in dealing in the information age."*
>
> **General Joseph Dunford**
> **Chairman of the Joint Chiefs of Staff**
> **15 February 2016 News Conference**

1. Joint Planning Process and Cyberspace Operations

a. Commanders integrate CO into their campaigns and operations at all levels. Their plans should address how to effectively integrate cyberspace capabilities, counter adversaries' use of cyberspace, identify and secure MRT-C, access key terrain in cyberspace, operate in a denied environment, efficiently use limited cyberspace assets, and pair operational requirements with cyberspace capabilities. The commander provides initial planning guidance, which may specify time constraints, outline initial coordination requirements, authorize the movement of forces within the commander's authority, and direct other actions as necessary. Supporting CO plans and concept of operations (CONOPS) describe the role and scope of CO in the commander's effort and address how CO support the execution of the supported plan. If requested by a commander, CDRUSCYBERCOM provides assistance, via the supporting CO-IPE, in integrating cyberspace forces and capabilities into the commander's plans, orders, and assessments.

b. CDRUSCYBERCOM plans, executes, and assesses CO based on a strategic approach of persistent engagement in cyberspace, employing a continuous operational tempo to seize and maintain the initiative required to compete and to set favorable security conditions in and through the IE that secure, defend, and advance US strategic goals. CO plans focus on adversary and enemy decision making, precluding their options, constraining their ability to maneuver, forcing them to react to friendly actions, and shaping their impressions. Effective CO plans seek to exploit adversary vulnerabilities while reducing our own, creating effects inside and outside of cyberspace that advance US goals across the competition continuum.

c. JP 5-0, *Joint Planning,* describes the joint planning process (JPP) as a proven process to organize the work of the commander, staff, subordinate commanders, and other partners to develop plans that appropriately address the problem to be solved. It focuses on framing the situation and end states, defining the military mission, analysis of critical factors, and designing both an operational approach to achieve mission objectives and an assessment framework to monitor the efficacy and progress of that accomplishment. CO capabilities and functions are integrated along with all other joint capabilities and functions into the JPP.

2. Cyberspace Operations Planning Considerations

a. **Overview.** Although CO planners are presented the same operational design considerations and challenges as planners for operations in the physical domains, there are some unique considerations for planning CO. For instance, because of unforeseen linkages in cyberspace, higher-order effects of some CO external missions may be difficult to predict. This may require extensive branch and sequel planning. Further, while many elements of cyberspace can be mapped geographically, a full understanding of an adversary's disposition and capabilities in cyberspace involves understanding the target, not only at the underlying physical network layer but also at the logical network layer and cyber-persona layer, including profiles of system users and administrators and their relationship to adversary critical factors. For planning internal operations within DOD cyberspace, DODIN operations and DCO-IDM planners require a clear understanding of the alignment of DODIN areas of operations and sectors and their assigned protection priorities based on mission-essential tasks and identification of MRT-C; which friendly forces or capabilities might be targeted by an adversary; what DODIN vulnerabilities are most likely to be targeted and the potential effects of the adversary's action; and the applicable domestic, foreign, and international laws and USG policy. Threats in cyberspace may be nation-states, non-state groups, or individuals, and the parts of cyberspace they control are not necessarily within the geographic borders associated with the threat's nationality or proportional to their geopolitical influence. A criminal element, a politically motivated group, or even a well-resourced individual may have a greater presence and capability in cyberspace than do many nations. Moreover, many adversaries operate cyberspace capabilities from portions of cyberspace geographically associated with the United States or owned by a US entity. Finally, the sensitive nature of planning and assessment of CO can lead to its segregation from planning and assessment of operations in the physical domains, thereby inhibiting effective cross-domain integration and synchronization of mutually supporting actions and their cross-domain effects. Each of these factors complicates the planning of CO.

b. **Planning Timelines.** For external missions, it is essential that OCO and DCO-RA planners understand the authorities required to execute the specific CO actions proposed. The applicable authorities may vary depending upon the phase of the operation. This includes accounting for the lead time required to obtain the necessary intelligence to define the correct target; develop target access; confirm the appropriate authorities; complete necessary coordination, including interagency coordination, deconfliction, and/or synchronization; and to verify the cyberspace capability matches the intended target using the results of technical assurance evaluations. A network engagement approach to planning external missions can help CO planners understand different layers or networks in relationship to one another, leverage partner capabilities, and assess potential vulnerabilities. Early and continuous coordination with interagency and international partners can expedite resolution of interagency and international partner issues, while potentially enabling the discovery of additional options. The internal missions of DODIN operations and DCO-IDM are conducted continuously across the competition continuum as an enduring campaign. For internal missions, the timelines for planners are impacted by other factors, including levels of automation available to manage network posture, availability of security solutions from commercial providers and their licensing requirements, and operational considerations that may impact a defender's ability to maneuver or take systems off-line to better manage their protection. However, the planning fundamentals remain the same, and despite the additional considerations and challenges of integrating CO, planners use the JPP to implement the commander's intent and guidance.

c. **Planning Considerations for Operating in Red and Gray Cyberspace**

(1) **Coordination of CO Missions.** CDRUSCYBERCOM exercises coordinating authority for planning and is responsible for executing global CO, as directed. This coordination is synchronized within the global integration frameworks approved by the CJCS and is conducted IAW CJCS-issued EXORDs, including those for C2 of CO, for global ISR in cyberspace, and for global competition. These orders clarify the relationships and coordination requirements for CDRUSCYBERCOM and CCDRs to whom the support is being provided or within whose AOR the effects in cyberspace are created. Additionally, close coordination and deconfliction between CO external and internal missions prevent unintentional conflicts between mission types and improve DODIN protection planning in anticipation of predicted cyberspace threats.

(2) **Characteristics of Cyberspace Capabilities.** While cyberspace is complex and ever changing, the JFC relies on cyberspace capabilities, whether devices or computer programs, to create the intended effects. However, cyberspace capabilities are developed based on environmental assumptions and expectations about the operating conditions that will be found in the OE. These conditions may be as simple as the type of computer operating system being used by an adversary or as complex as the exact serial number of the hardware or version of the software installed, what system resources are available, and what other applications are expected to be running (or not running) when the cyberspace capability activates on target. These expected conditions should be well documented by the capability developer and are important for planners and targeting personnel to understand as capability limitations. The extent to which the expected environmental conditions of a target cannot be confirmed through ISR represents an increased level of risk associated with using the capability. All other factors being equal, cyberspace capabilities that have the fewest environmental dependencies and/or allow the operator to reconfigure the capability are preferred. DODI O-3600.03, *Testing and Evaluation of Cyberspace Effects and Enabling Capabilities,* provides detailed requirements for technical assurance evaluations that document these characteristics.

(3) **Cascading, Compounding, and Collateral Effects.** Overlaps among military, other government, corporate, and private activities on shared networks in cyberspace make the evaluation of probable cascading, compounding, and collateral effects particularly important when targeting for CO. The effects can ripple through an affected system, sometimes cascading through links with related systems that were not evident to the planner. Cascading effects sometimes travel through systems subordinate to the one

targeted but can also move laterally to peer systems or up to higher-level systems. Compounding effects are an aggregation of various levels of effects that have interacted in ways that may be intended or may have been unforeseen. Collateral effects, including collateral damage, are the incidental effects of military operations on persons and property that were not the intended targets of the action. Depending upon the strategic and operational situation, an order or applicable ROE may limit CO to only those actions likely to result in no or low levels of collateral effects. A collateral effects estimate to meet policy restrictions is separate from the proportionality analysis required by the law of war. This estimate is a tool for the commander to understand the risk of proposed operations. Therefore, even if a proposed CO collateral effects analysis is conducted, the likely effects of the proposed CO must also be permissible under a law of war proportionality analysis, and the CO must meet the requirements for taking feasible precautions to reduce the risk of incidental harm, as applicable.

(4) **Reversibility of Effects.** An important consideration for planning cyberspace attack and cyberspace exploitation effects is the level of control over the duration of the effect that can be exercised by friendly forces. There are two basic ways to categorize effects by this standard:

(a) **Operator Reversible Effects.** Effects that can be recalled, recovered, or terminated by friendly forces. Depending upon geopolitical conditions, these effects may represent a lower risk of undesired consequences, including discovery or retaliation.

(b) **Non-Operator Reversible Effects.** Effects that cannot be recalled, recovered, or terminated by friendly forces after execution. These effects may represent a higher risk of response from the threat or other undesired consequences and may require more coordination.

See Appendix A, "(U) Classified Planning Considerations for Joint Cyberspace Operations," for additional planning considerations for external missions. See JP 3-60, Joint Targeting, *for additional information on creation of effects. Refer to CJCSI 3160.01,* (U) No-Strike and the Collateral Damage Estimation Methodology, *for additional information on collateral damage.*

d. **Planning Considerations for Protecting the DODIN**

(1) **For Specific Campaigns and Operations.** DODIN operations underpin nearly every aspect of military operations, and this reliance on cyberspace is well understood by our adversaries. A commander's reliance on specific segments of the DODIN is often not considered during plans development, but planning for DODIN resiliency is essential. Planning staffs should incorporate branches and sequels for any operations that pose an increased threat to the DODIN, defining primary and alternate means from which to execute mission-essential tasks or functions. This planning occurs with the expectation that the associated MRT-C will be protected; however, branch planning should consider alternate outcomes. The CCDR's CO staff coordinates and deconflicts any locally performed DCO-IDM mission activities with JFHQ-DODIN. If the

planned cyberspace defense actions will create effects in cyberspace outside of the CCDR's AOR, JFHQ-DODIN ensures their global coordination and synchronization.

(2) **Prioritizing DODIN Protection.** Cybersecurity policies and standards generally apply to all of the DODIN and create a level of consistency for the static security posture of DOD cyberspace. These standards do not necessarily reflect the current priorities of commanders who operate or depend upon networks. Operational commanders are responsible for managing cyberspace threat risk to their mission if they grant waivers or exceptions to cybersecurity policy implementation. But most risk from cyberspace threats cannot be managed from the perspective of a single commander, so these waivers are granted in consultation with JFHQ-DODIN and other users who may be impacted by shared risk. Each sector of the DODIN has an organization responsible for its security and first-line defensive actions, including administrative and non-mission-critical networks, which are protected primarily by their operators and their CSSP. Some of these protection services may be contracted, particularly when the creation and operation of the network itself has been contracted. The determination of whether or not a specific piece of contractor hardware or a specific contractor network segment is considered part of the DODIN is determined by the exact language of the contract. Given the limited number of CPTs and other cyberspace forces, the significant scope of the DODIN means it cannot all be defended in the same depth. Protection of DODIN sectors is prioritized based on mission-essential tasks, with CPTs augmenting the efforts of in-place defense when appropriate.

(3) **Coordinating DODIN Defense.** Effective response to intrusions or other MCA on the DODIN requires coordinated action at the tactical, operational, and strategic levels. Although the ultimate goal of DCO is to defeat the threat and reestablish secure cyberspace, the nature of the threat determines the specific response to each incident. Response to threat activity on the DODIN is normally either triggered by tactical information or derived from sensors; local analysis; or intelligence, LE, or CI reporting. All cybersecurity incidents are reported IAW DOD policy, and some MCA may be effectively remediated by well-trained, local cyberspace forces without external support or reinforcement. JFHQ-DODIN informs USCYBERCOM and all impacted DODIN sectors about threat status and directs appropriate responses based on the scope of the threat. Sophisticated nation-state threats require a different type of response. Each encounter with a peer or near-peer adversary in cyberspace warrants careful consideration of the response. Choosing when, where, and how to engage the threat is as important in DCO as it is to defense in the physical domains. If circumstances allow, including a consideration of threat to the supported mission, intelligence gain/loss (IGL) considerations may suggest careful observation of the threat while limiting its maneuver. When a command is engaged with a threat in cyberspace, the global enterprise adapts to support that command IAW defensive priorities. Reachback support for analytics, intelligence, and even fires is provided to maintain continuity of operations at the supported command. Some incidents require remote or expeditionary response by CPTs to reinforce network operators and the assigned CSSP to defeat the threat and re-secure the affected segment of cyberspace.

(4) **Situational Awareness.** Cyberspace situational awareness is the requisite current and predictive knowledge of cyberspace and the OE upon which CO depend, including all factors affecting friendly, adversary, and enemy cyberspace forces. A commander continually assesses the OE through a combination of staff element and other reporting; personal observation; intelligence, to include threat warning; and representations of various activities occurring in the OE using a common operational picture (COP). The DODIN is a primary source of information used to support the commander's situational awareness of the OE, including the status of the DODIN itself. Sustainment of DODIN sensors, communication channels, data feeds, and user interfaces is a key outcome of DODIN operations. Accurate and comprehensive situational awareness is critical for rapid decision making in a constantly changing OE and while engaging an elusive, adaptive enemy. Situational awareness of adversary and enemy activity in gray and red cyberspace relies heavily on cyberspace exploitation and SIGINT, but contributions can come from all sources of intelligence. Situational awareness within the DODIN is provided by the Services and agencies operating their portions of the DODIN, including CSSPs, by DISA and JFHQ-DODIN through the network operations and security centers, by USCYBERCOM's Joint Operations Center, and by the SATCOM Integrated Operations Division of United States Space Command's Combined Space Operations Center. They coordinate with each other as required for operational effectiveness and shared situational awareness. The ever-increasing complexity and scope of cyberspace means a commander never has perfect or even optimal situational awareness of cyberspace factors that could impact operations and should consider the risks represented by this lack of information when making decisions.

e. **Preparing for Assessment.** Assessment measures progress of the joint force toward mission accomplishment. Commanders continuously assess the OE and the progress of operations and compare them to their initial vision and intent. The assessment process begins during planning and helps the commander and staff decide what to measure and how to measure it, to determine progress toward accomplishing a task, creating an effect, or achieving an objective. The data collected to support these measures can range from simply noting an inability to reach the target network after a cyberspace attack to complex network monitoring and statistical analysis. Data gathered about the target's state prior to the operation, through access, execution, and possibly its long-term post-attack state, may facilitate later assessment of higher-order effects. Assessment of internal missions to protect the DODIN requires similar preparation. It is difficult to determine the degree that protection measures reduce risk to mission without accurate knowledge of the initial conditions of the network. Assessment of CO is not limited to analysis of data from within cyberspace. For example, if the desired effect of an OCO mission was to cause a power outage, the assessment might be made using visual sensors to observe indications of an outage. Planners submit assessment requests with sufficient justification, as early as is necessary for the appropriate allocation of resources and for the timely collection of pre-execution baseline data for later comparison. For further information, see paragraph 7, "Assessment of Cyberspace Operations."

Refer to Appendix A, "(U) Classified Planning Considerations for Joint Cyberspace Operations," for additional information on planning CO.

3. Intelligence and Operational Analytic Support to Cyberspace Operations Planning

a. **Priority Intelligence Requirements (PIRs).** During mission analysis, the joint force staff identifies PIRs about the threat and other relevant aspects of the OE. Based upon the PIRs, the intelligence staff develops more specific essential elements of information (EEIs), indicators, and specific information requirements to inform CCDR decision making. Information requirements related to cyberspace can include such things as network infrastructures and status, readiness of the threat's equipment and personnel, and unique cyberspace signature identifiers such as hardware/software/firmware versions and configuration files. The resulting requirements are met through a combination of military intelligence and national intelligence sources, including open sources.

(1) **Requests for Information (RFIs).** CO planners can submit an RFI for consideration to the intelligence staff. RFIs are specific, time-sensitive, ad hoc requirements for information to support an ongoing crisis or operation. Once validated against standing and ad hoc PIRs/EEIs, the CCMD may decide to collect intelligence and/or produce intelligence products in support of the RFI. RFIs fulfill customer requirements and range from disseminating existing products through integrating or tailoring on-hand information to scheduling new collection and production. In addition to information collected during military operations, information required to support CO planning can come from SIGINT, human intelligence, CI, measurement and signature intelligence, geospatial intelligence, or open-source intelligence (OSINT). Regardless of source, the information should be timely, relevant, accurate, and in a usable format.

(2) **Intelligence Architecture.** The DOD's global connectivity enables commanders to task assigned or attached ISR sensors or ISR-capable units and submit collection and production requirements directly to other ISR or IC activities. For more information on this architecture and on PIRs and RFIs, see JP 2-0, *Joint Intelligence.*

b. **Threat Detection and Characterization.** Some threats in cyberspace are detected by intelligence sources and others during the course of military maneuver.

(1) **Detection.** The activities in cyberspace of a sophisticated threat may be difficult to detect. Unlike actions in the physical domains, which are often detected by the presence of military equipment or other types of observables, threat actions in cyberspace may not be easily distinguishable from legitimate network activity. The ability to detect threat activities in cyberspace is critical for enabling effective CO.

(2) **Characterization.** Because the DOD CO missions are categorized based on the commander's intent and because friendly forces are often uncertain of a threat's actual intent, threat activities in cyberspace are referred to more generically as MCA. If known details of adversary or enemy activity support more precise categorization, specific threat actions should be described using specific effects terminology.

(3) **Analysis and Attribution.** Due to the characteristics of the physical network, logical network, and cyber-persona layers of cyberspace, attribution of MCA to a specific person, criminal organization, non-state threat, or even a responsible nation-state can be exceptionally difficult. Although attribution is not necessarily required for self-defense, the difficulty of attribution, along with the possibility that an apparent threat may actually be an attempt at misdirection, is one of the principal reasons DCO-RA mission planning may be more difficult than planning for response to conventional attack. The risks of a defensive response against the wrong threat, particularly a nation-state or a target within an unwitting nation-state where the attack originated, are weighed against strategic objectives and the consequences of making an attribution mistake. Working effectively within these constraints requires unique skills on the part of all-source intelligence analysts to understand the context of the threat activity. They use skills like analyzing deception techniques, anonymity techniques, virtual representations and avatars, and other artifacts of the logical network and cyber-persona layers to characterize activities with the requisite degree of confidence required to enable an effective response.

c. **IGL.** Another planning concern is that maneuver and fires in red and gray cyberspace could potentially compromise intelligence collection sources and methods. To the maximum extent practicable, an IGL assessment is required prior to executing such actions. The IGL assessment and stakeholder equity deconfliction are conducted IAW national policy guidance and can be complicated by the array of non-DOD USG and multinational partners operating in cyberspace. JFCs use IGL analysis to weigh the risks of conducting the CO versus achieving the desired objective via other methods.

d. **Warning Intelligence.** Cyberspace threat intelligence includes all-source analysis to factor in political, military, and technical warning intelligence. Adversary and enemy cyberspace actions may occur separate from, and well in advance of, related activities in the physical domains. Additionally, cyberspace threat sensors may recognize MCA with only a very short time available to respond. These factors make the inclusion of all-source intelligence analysis very important for effectively assessing adversaries' intentions in cyberspace.

e. **OSINT.** All-source intelligence analysis of cyberspace sources should take advantage of the information available from OSINT, including Internet social media and other nontraditional sources of information. The constantly evolving sphere of open-source activity offers the opportunity to add useful data to all-source analysis. But this constantly changing landscape of media and the often low quality of data available in cyberspace also complicate the intelligence collection problem, requiring active collection management to stay abreast of these sources.

f. **ISR.** ISR is an activity that synchronizes and integrates the planning and operation of sensors; assets; and processing, exploitation, and dissemination systems in direct support of current and future operations. This is an integrated intelligence and operations function. ISR conducted in cyberspace is part of a CO external mission and focuses on gathering tactical and operational information required for targeting or intelligence on adversary and enemy networks to support military planning. To optimize use of all available ISR assets, an ISR CONOPS should be developed, in conjunction with the command's overall intelligence planning effort that includes collection in cyberspace. This CONOPS should be based on the collection strategy and ISR execution planning and should be developed jointly by the joint force intelligence directorate of a joint staff and the operations directorate of a joint staff. It outlines the capability to task, collect, process, exploit, and disseminate accurate and timely information from and about cyberspace that provides the awareness necessary to successfully plan and conduct operations. It addresses how all available ISR collection assets and associated processing, exploitation, and dissemination infrastructure, including multinational and commercial assets, will be used to satisfy the joint force's anticipated collection tasks. It also requires appropriate deconfliction and personnel who are trained and certified to a common standard with IC personnel.

Refer to Appendix A, "(U) Classified Planning Considerations for Joint Cyberspace Operations," for additional information on types of ISR conducted in cyberspace and related authorities.

4. Joint Targeting

The purpose of joint targeting is to integrate and synchronize fires into joint operations. Joint targeting is the process of selecting and prioritizing targets and matching the appropriate capability to them, considering operational requirements. Integrating and synchronizing planning, execution, and assessment are pivotal to the success of joint targeting. The overall joint targeting cycle and target development process described in JP 3-60, *Joint Targeting,* apply generally to targeting in support of CO. In addition, the coordination required by Chairman of the Joint Chiefs of Staff Manual (CJCSM) 3139.01, *(U) Review and Approval Process for Cyberspace Operations,* for certain OCO and DCO-RA missions, is unique to CO and applies to many aspects of the joint targeting cycle. Therefore, CO planners and decision makers often use a targeting process specifically adapted to their circumstance. Some characteristics unique to the cyberspace components of targets and to cyberspace capabilities are described below.

a. **Joint Targeting In and Through Cyberspace.** Planning and targeting staffs develop and select targets in and through cyberspace based on the commander's objectives rather than on the capabilities available to achieve them. The focus is on creating effects that accomplish targeting-related tasks and that support achievements of objectives, not on using a particular cyberspace capability simply because it is available. Targets that can be accessed in cyberspace are developed, vetted, and validated within the established joint targeting process. Specific considerations for joint targeting in and through cyberspace include that:

(1) Cyberspace capabilities are a viable option for engaging some targets;

(2) For some targets, using a cyberspace capability may be the preferred approach, since they may offer low probability of detection and/or no associated physical damage;

(3) Higher-order effects on targets in cyberspace may ultimately impact elements of the DODIN (e.g., taking out a key Internet node upon which an enemy and the DODIN both rely); and

(4) Planning cross-domain synchronization of fires requires consideration of security classifications of some cyberspace capabilities.

b. Although targets paired with cyberspace capabilities can often be engaged with no permanent damage, due to the interconnectedness of cyberspace, the effects of CO may cross geographical boundaries and, if not carefully planned, may have unanticipated effects. As a result, engaging targets in and through cyberspace requires close coordination within DOD and with interagency and multinational partners. Every target has distinct intrinsic or acquired characteristics (i.e., physical, functional, cognitive, environmental, and temporal) that form the basis for detection, location, and identification; for determining target value within the target system; and for classification for future surveillance, analysis, strike, and assessment. The challenge in joint targeting for CO is to identify, correlate, coordinate, and deconflict multiple activities occurring across the physical network, logical network, and cyber-persona layers. This requires a C2 capability that can operate at the tempo of CO and can rapidly integrate impacted stakeholders.

(1) **Physical Network Layer Target Features.** The physical network layer is the medium where the data travels. It includes wired (e.g., land and undersea cable) and wireless (e.g., radio, radio-relay, cellular, satellite) transmission means. It is a point of reference for determining geographic location and the applicable legal framework.

(2) **Logical Network Layer Target Features.** The logical network layer provides an alternate view of the target, abstracted from its physical location, and referenced from its logical position in cyberspace. This position is often represented through a network address (e.g., IP address). It depicts how nodes in the physical domains address and refer to one another to form entities in cyberspace. The logical network layer is the first point where the connection to the physical domains may be lost. Joint targeting in the logical layer requires the logical identity and logical access to the target to have a direct effect.

(3) **Cyber-Persona Layer Target Features.** The cyber-persona layer, the aggregate of an individual or group's identity(ies) in cyberspace and an abstraction of logical network layer data, holds important implications for joint forces in terms of positive target identification, affiliation, and activity attribution. Cyber-personas are created to group information together about targeted actors to organize analysis, planning, and intelligence reporting. Because cyber-personas can be complex, with elements in many virtual locations but often not linked to a single physical location or form, sufficient intelligence collection and analysis capabilities are required for the joint forces to gain insight and situational awareness required to enable effective joint targeting of a cyber-persona. Ultimately, cyber-personas must be linked to features that can be engaged in either the logical or physical network layers.

c. **Target Access.** Cyberspace forces develop access to targets or target elements in cyberspace by using cyberspace exploitation actions. This access can then be used for various purposes, ranging from information collection to maneuver and to joint target nomination. Not all accesses are equally useful for military operations. For instance, the level of access required to collect information from a targeted system may not be sufficient to create a cyberspace attack effect. Developing access to targets in or through cyberspace follows a process that can often take significant time. In some cases, remote access is not possible or preferable, and close proximity may be required, using expeditionary CO. Such operations are key to addressing the challenge of closed networks and other systems that are virtually isolated. Expeditionary CO are often more regionally and tactically focused and can include units of the CMF or special operations forces. All target access efforts in cyberspace require coordination with the IC for deconfliction IAW national policy and to illuminate potential IGL concerns. If direct access to the target is unavailable or undesired, sometimes a similar or partial effect can be created by indirect access using a related target that has higher-order effects on the desired target. Some denial of service cyberspace attacks leverage this type of indirect access.

d. **Target Development, Nomination, and Synchronization.** CO use standard target nomination processes, but target folders should include unique cyberspace aspects (e.g., hardware and software configurations, IP address, identifying features of a cyber-persona) of the target. Development of this data is imperative to understand and characterize how elements targetable through cyberspace are relevant to the commander's objective. This data also enables the planner to match an appropriate cyberspace capability against a particular target. Component commanders, national agencies, supporting commands, and/or the JFC planning staff nominate targets to the targeting staff for development and inclusion on the joint target list (JTL). Once placed on the JTL, JFCs in receipt of an EXORD with relevant objectives and ROE can engage the target with organic forces (if within a component commander's assigned area of operations and consistent with any restrictions) or nominate the target to CDRUSCYBERCOM for action by other joint force components and other organizations. For pursuing targets with a global presence, some CCDRs also maintain globally integrated target lists to enable more effective coordination across AORs.

e. **Time-Sensitive Targets (TSTs)**

(1) A TST is a validated joint target of such high priority to friendly forces that the commander designates it for immediate engagement because it poses (or will soon pose) a threat to friendly forces or is a highly lucrative, fleeting target. TSTs are normally engaged dynamically. However, to be successfully engaged, they require considerable planning and preparation within the joint targeting cycle. Engaging TSTs in cyberspace is difficult in most situations, because they are likely to cross AORs and require detailed joint, interagency, and/or multinational planning efforts.

(2) Being prepared to engage a TST from within cyberspace requires early coordination between CO planners, operators, and the supported commander to ensure an appropriate cyberspace capability and required access are available. Successful

prosecution of TSTs in cyberspace requires a well-organized and well-rehearsed process for sharing sensor data and target information, identifying suitable strike assets, obtaining mission approval, and rapidly deconflicting cyberspace capability employment. These challenges should be considered when developing the TST matrix.

See JP 3-60, Joint Targeting, *for additional information on joint targeting and JP 2-0,* Joint Intelligence, *for additional information on intelligence operations.*

Refer to Appendix A, "(U) Classified Planning Considerations for Joint Cyberspace Operations," for additional information on intelligence support to planning CO.

5. Command and Control of Cyberspace Forces

a. Clearly established command relationships are crucial for ensuring timely and effective employment of forces, and CO require unity of command and unity of effort. However, the complex nature of CO, where cyberspace forces can be simultaneously providing actions at the global level and at the theater or JOA level, requires adaptive C2 structures. Joint forces principally employ centralized planning with decentralized execution of operations. CO require constant and detailed coordination between theater and global operations, creating a dynamic C2 framework that can adapt to the constant changes, emerging threats, and unknowns. Certain CO functions, including protection of the DODIN against global cyberspace threats, lend themselves to centralized planning and execution to meet multiple, near-instantaneous requirements for response. Centrally controlled CO should be integrated and synchronized with the CCDR's regional or local CO, conducted by forces assigned to, attached to, or in support of the CCDR, as directed in the *(U) Global Force Management Allocation Plan* (GFMAP). For these reasons, there may be times when C2 of forces executing simultaneous global CO and theater CO is conducted using supported/supporting command relationships under separate, but synchronized, chains of command. CO are integrated and synchronized by the supported commander into their CONOPS, detailed plans and orders, and specific joint operations.

b. **C2 for Global CO.** CDRUSCYBERCOM is the supported commander for transregional and global CO and manages day-to-day global CO even while acting as supporting commander for one or more CCDR's operations. For a specific CO mission, the support relationships are established in an EXORD, OPORD, or establishing directive. A supported relationship for CO does not exempt either command from coordinating actions with affected commanders prior to conducting an operation. Regardless of the approach employed for any particular operation, unless otherwise specified by the President or SecDef, C2 for CO is implemented IAW current CJCS CYBER C2 EXORD and other relevant orders to help ensure effective coordination and synchronization of joint forces and to provide a common construct for JFCs to execute their mission within a global context. JFHQ-DODIN centrally coordinates and directs global DODIN operations and DCO-IDM when these operations have the potential to impact the integrity and operational readiness of multiple DOD components. Although execution of many actions may be decentralized, CDRUSCYBERCOM is the supported commander for CO to secure, operate, and defend the DODIN and, when ordered, to defend other US critical cyberspace assets, systems, and functions. As the DODIN continues to migrate toward a common architecture standard, routine cyberspace security actions for global networks will continue shifting to centralized locations, such as the JFHQ-DODIN Operations Center.

c. **C2 for CO Supporting CCMDs.** CCDRs are supported for CO in their AOR or for their transregional responsibilities, with CDRUSCYBERCOM supporting as necessary. These CO comprise actions intended to have effects localized within a CCDR's AOR or a transregional functional responsibility. These could be cyberspace security and defense actions internal to a theater DODIN segment or external actions, such as cyberspace exploitation or cyberspace attack against a specific enemy capability. In addition to the theater segments of global networks, CCMD-level DODIN operations and DCO-IDM include the protection of stand-alone and tactical networks and computers used exclusively by the CCMD. For example, CCMD-level maneuvers in cyberspace include activities to reposition capabilities to enhance threat detection in specified areas, to focus cyberspace forces activity in areas linked to specific operational branches and sequels to keep the adversary at risk, or to activate stand-by tactical cyberspace capabilities to transition friendly C2 to more secure locations. Such CO maneuvers are vital when a CCDR's systems are under attack to the degree that subsets of the DODIN are degraded, compromised, or lost. In such operations, the supported CCDR coordinates, through their USCYBERCOM CO-IPE, with the associated theater network operations and security center, supported by JFHQ-DODIN and DISA, to restore the affected cyberspace. The supported CCDR also integrates, synchronizes, and normally directs CO actions in red and gray cyberspace, including fires, with other lethal and nonlethal effects, for which they may use assigned, attached, or supporting cyberspace forces. CCDRs develop and coordinate their requirements for such effects with the CO-IPE and supporting JFHQ-C, for deconfliction and prioritized execution. When a CCDR establishes a subordinate force (e.g., a JTF), the cyberspace unit(s) assigned to support that force is(are) determined by the CCDR's mission requirements in coordination with CDRUSCYBERCOM.

d. **Specific Relationships for USCYBERCOM C2 of Cyberspace Forces.** SecDef establishes relationships for C2 of the CMF via CJCS EXORD. These relationships are described below and depicted graphically in Figure IV-1.

(1) USCYBERCOM C2 relationships:

(a) CDRUSCYBERCOM has COCOM of all GFMIG-assigned cyberspace forces.

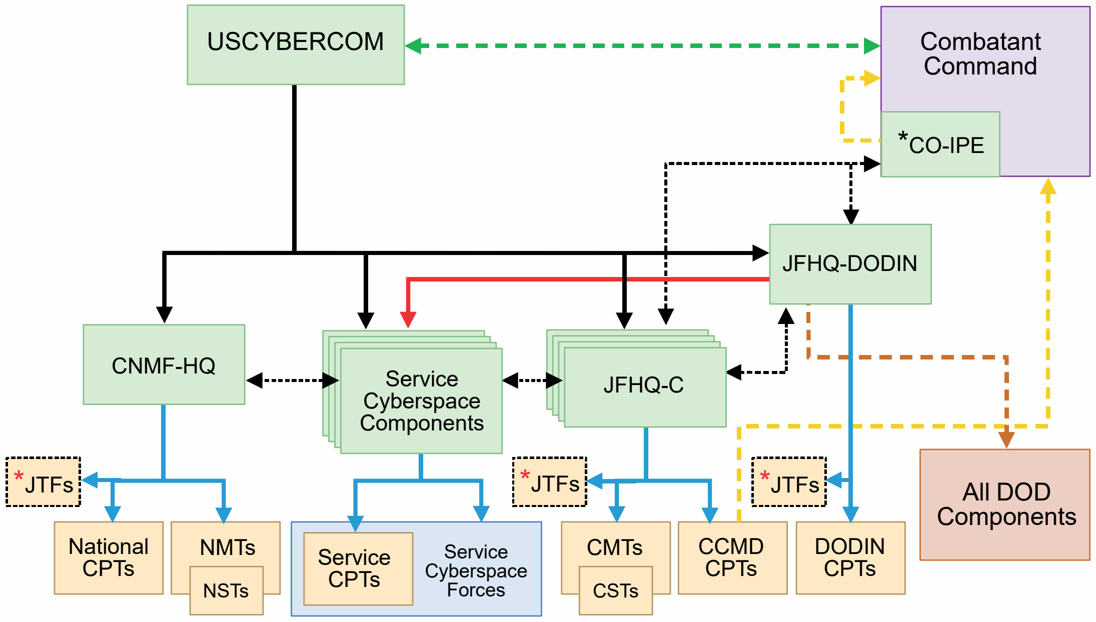
(b) CDRUSCYBERCOM has support relationships with all other CCDRs.

(c) CNMF commander has OPCON of NMTs/NSTs and national CPTs.

(d) JFHQ-C commanders have OPCON of CMTs, CSTs, and CCMD CPTs and direct the activities of the CO-IPEs.

(e) JFHQ-DODIN commander has OPCON of DODIN CPTs and directs the activities of the United States Transportation Command (USTRANSCOM) CO-IPE.

Command and Control of the Cyber Mission Force



* CO-IPE is provided by USCYBERCOM in direct support of combatant commander. All CO-IPEs are OPCON to JFHQ-Cs except the USTRANSCOM CO-IPE, which is OPCON to JFHQ-DODIN.

* JTFs are commonly established to accomplish emergent or enduring CO mission requirements.

Legend

CCMD	combatant command
CMT	combat mission team
CNMF-HQ	Cyber National Mission Force Headquarters
CO	cyberspace operations
COCOM	combatant command (command authority)
CO-IPE	cyberspace operations-integrated planning element
CPT	cyberspace protection team
CST	combat support team
DACO	directive authority for cyberspace operations
DOD	Department of Defense
DODIN	Department of Defense information network
JFHQ-C	joint force headquarters-cyberspace
JFHQ-DODIN	Joint Force Headquarters-Department of Defense Information Network
JTF	joint task force
NMT	national mission team
NST	national support team
OPCON	operational control
TACON	tactical control
USCYBERCOM	United States Cyber Command
USTRANSCOM	United States Transportation Commad

⟶	COCOM
⟶	OPCON
⟶	TACON
⇢	DACO
⇢	supporting/ supported
⇢	direct support
⇢	coordination

Figure IV-1. Command and Control of the Cyber Mission Force

(f) JFHQ-DODIN commander has tactical control of SCC commands for DODIN operations and DCO-IDM only.

(g) JFHQ-DODIN commander has DACO, delegated from CDRUSCYBERCOM, over all DOD components for global DODIN operations and DCO-IDM.

(h) SCC commanders have OPCON of Service CPTs and other forces attached by CDRUSCYBERCOM (e.g., CSSPs).

(i) SCC commanders have DACO, delegated from CDRUSCYBERCOM, over all related Service components for DODIN operations and DCO-IDM.

(2) CCMD C2 relationships:

(a) CCDRs have COCOM of cyberspace forces assigned in the GFMIG and command allocated cyberspace forces as described in the GFMAP.

(b) SecDef establishes support relationships between CCDRs for CO.

(c) JFHQ-C commanders support CCMDs using general support for OCO and direct support for DCO-IDM.

(d) USCYBERCOM CO-IPEs provide direct support to CCDRs as a subordinate element of the CCDR's supporting JFHQ-C, except in the case of USTRANSCOM, whose CO-IPE is subordinate to JFHQ-DODIN.

(3) When CCDRs have CO requirements that exceed their capacity or authority, they request support through the following processes, established in the CJCS CYBER C2 EXORD:

(a) Requirements for CPF direct support. CCMDs request CPF direct support through the standard global force management process with a request for direct support IAW the GFMIG and CJCSM 3130.06, *(U) Global Force Management Allocation Policies and Procedures.* CDRUSCYBERCOM delegates OPCON of CCMD CPTs to a subordinate JFHQ, which places them in direct support of a specific CCMD as required. CPTs allocated in direct support to a CCMD remain OPCON to CDRUSCYBERCOM unless otherwise directed by SecDef.

(b) Requirements for CO external mission support. CCMDs request OCO or DCO-RA support via their supporting JFHQ-C, which coordinates with other USCYBERCOM components as required.

(c) Requirements for cyberspace-enabled activities. CCMDs' requirements for forces already assigned through the GFMIG process—outside of the CPF, CNMF, or CCMF—to plan or execute cyberspace-enabled activities (e.g., MISO or CI support) submit a request for forces through the GFMAP as per CJCSM 3130.06, *(U) Global Force Management Allocation Policies and Procedures.* Unless otherwise directed by SecDef, OPCON of allocated forces transitions to the requesting CCDR only when ordered in the GFMAP.

(d) Requirements for special technical operations support. CCMDs that require special technical operations support in cyberspace submit requests using the integrated joint special technical operations (IJSTO) process.

(4) **Mission-Tailored Forces.** CDRUSCYBERCOM and commanders of CMF units tailor their assigned cyberspace forces, additional CO support personnel, and

cyberspace capabilities as required to support mission requirements. These tailored forces can take a variety of forms, from a small CPT mission element to a named JTF. They are task-organized and operate for the duration of the crisis/contingency or other operation or until redeployed by CDRUSCYBERCOM in coordination with the supported CCDR. In addition to USCYBERCOM/CMF elements, the Services and United States Special Operations Command tailor retained/assigned cyberspace forces as required to support mission requirements.

e. **C2 for CO Internal and External Missions.** The nature of C2 relationships for CO varies, depending upon whether they are internal to DODIN or other blue cyberspace or they are external missions in gray or red cyberspace.

(1) **CO Internal Missions.** C2 of forces conducting DODIN operations and DCO-IDM may require preplanned and preauthorized actions based on particular conditions and triggers, executed either manually or automatically, depending upon the nature of the threat and urgency of the required action. The commander's operations and planning staff should understand the interrelationships of the cyberspace they are protecting, how the appropriate capabilities can be effectively employed to defeat threats, and, when necessary, how to deconflict cyberspace defense actions with the mission-critical operations that cannot be interrupted. Cyberspace forces defending CCMD segments of the DODIN may be geographically separated from the supported theater of operations. For example, forces conducting remote actions in support of DCO-IDM often simultaneously support defense of cyberspace in multiple geographic locations. This requires extensive coordination, planning, and early integration of requirements and capabilities. Such cases require all involved commanders to take extra measures so the supported commander is continuously aware of the remote supporting forces' operational status. In other cases, CPTs may be deployed for expeditionary CO to specific locations where they are placed in direct support to local commanders to defend threatened cyberspace. In other cases, where there is no local military commander, for instance, when a CPT is deployed to support a DOD agency, all C2 authorities remain with the CPT's commander. Supported and supporting commanders coordinate the deployment and employment of cyberspace forces required to accomplish the assigned mission.

(2) **CO External Missions.** C2 relationships established to execute OCO and DCO-RA missions, which involve actions in gray and red cyberspace, require careful consideration of projected effects and geopolitical boundaries. The reliance of the global population on the interconnectivity of cyberspace requires carefully controlling the effects created during OCO and DCO-RA missions, with detailed planning, in-depth intelligence support, and national-level deconfliction to ensure appropriate consideration of nonmilitary factors such as foreign policy implications. Some of these CO external missions require centralized execution by CMTs or NMTs to create transregional effects. For example, a DCO-RA mission employing external countermeasures in multiple AORs to counter a large botnet (a network of computers linked together by malware) or actions, up to and including pre-emption, to block enemy cyberspace attack command signals directed from one AOR at another. Other external missions may be more regionally and tactically focused and use expeditionary cyberspace forces. When directed, CCDRs control

operations in and through cyberspace when there is confidence that effects are limited to their geographic AOR. Such authorities require CCDRs to remain cognizant of national cyberspace policy and its application to their plans and operations.

(3) Based on the nature of CO, the cyberspace C2 framework is adjusted for flexible and agile C2 of cyberspace forces to ensure US freedom of action in cyberspace while denying adversaries the same. For additional details beyond those discussed here, refer to the applicable CJCS EXORD and other relevant orders authorizing CO.

f. **Enabling C2 of Cyberspace Forces.** To provide effective C2 of forces conducting CO, several enabling factors are essential.

(1) **COP.** Despite the difficulties of achieving accurate and comprehensive situational awareness of all the aspects of cyberspace relative to a commander, the best available, real-time COP for cyberspace is important for effective C2 of forces executing CO. A COP of activities in cyberspace requires rapid fusion, correlation, and display of data from global network sensors to deliver a reliable picture of friendly, neutral, adversary, and enemy activity in all layers of cyberspace. In addition, an accurate cyberspace COP integrates real-time threat and event data from myriad sources (e.g., DOD enterprise operations centers and other service providers, IC, interagency partners, private industry, and international partners) and improves commanders' ability to identify, monitor, characterize, track, locate, and take action to engage targets or to respond to MCA. CDRUSCYBERCOM maintains global cyberspace situational awareness, and CCMDs maintain regional/functional cyberspace situational awareness along with an awareness of global factors in cyberspace that may impact operations in their theater/functional area.

(2) **Reach-Forward.** The complexity presented by cyberspace requires flexibility of forces and C2 to counter the broad variety of threats. Units of cyberspace forces providing global CO support may need to reach forward to support multiple CCMDs simultaneously. Allowing them to support CCMDs in this way permits faster adaptation to rapidly changing needs and allows threats that initially manifest only in one AOR to be mitigated globally in near real time. Likewise, while synchronizing CO missions related to achieving CCDR objectives, some cyberspace capabilities that support this activity may need to be forward-deployed; used in multiple AORs simultaneously; or, for speed in time-critical situations, made available via reachback. This might involve augmentation or deployment of cyberspace capabilities to forces already forward or require expeditionary CO by deployment of a fully equipped team of personnel and capabilities.

(3) **Reachback.** At the same time, CCMDs require the freedom and capability to effectively plan, coordinate, and conduct theater and functional CO. To enable these efforts, CO staff supporting CCDRs should understand how to arrange for timely and effective reachback support from USCYBERCOM and its subordinate units to augment the expertise and capacity of the supported commander.

(a) CCDRs size and structure their CO staff to best support their mission and requirements. This staff, supported by a USCYBERCOM CO-IPE, coordinates CO requirements and capabilities throughout their planning, intelligence, operations, assessment, and readiness processes to integrate and synchronize CO with other military operations. Additionally, as necessary and in partnership with USCYBERCOM, the CCMD coordinates CO regionally with interagency and multinational partners. Via their supporting JFHQ, the CCMD:

1. Combines inputs from USCYBERCOM with information about CCMD tactical and/or constructed networks to develop situational awareness and a COP tailored to CCMD requirements.

2. Facilitates, through USCYBERCOM, coordination and deconfliction of CCDR-directed CO, which may impact or conflict with other DOD or other USG cyberspace activities or operations within the AOR or functional area. As early as possible in the planning process, provides USCYBERCOM with sufficient information about CCDR-planned CO to enable deconfliction with other USG CO.

(b) USCYBERCOM CO-IPEs are organized to meet individual CCMD requirements and facilitate planning and coordination of all three cyberspace missions, as required. CO-IPEs remain in direct support of and are integrated with CCMD CO planning staff to provide a bridge for USCYBERCOM and its subordinate JFHQ to enable theater and global integration of cyberspace forces and operations.

g. **C2 of Multinational CO.** Although the US military will likely enter future conflicts as part of a multinational force (MNF), the level of integration of US cyberspace forces with foreign cyberspace forces varies depending upon in-place agreements with each partner and may not mirror the level of integration of other types of forces. Planning for the specific C2 elements desired by the US commander depends upon the type and scale of the operation, the cyberspace presence and sophistication of the adversary, and the types of targets identified. Regardless of which elements are established, the overlaps between global and theater missions in cyberspace, and relevant operational limitations, necessitate close coordination, and potentially, some level of integration, among CCDRs conducting multinational operations, CDRUSCYBERCOM, and other multinational and interagency partners. See paragraph 9, "Multinational Considerations," for additional information on multinational CO.

6. Synchronization of Cyberspace Operations

a. The pace of CO requires significant pre-operational collaboration and constant vigilance after initiation, for effective coordination and deconfliction throughout the OE. Keys to this synchronization are maintaining cyberspace situational awareness and assessing the potential impacts to the joint force of any planned CO, including the protection posture of the DODIN, changes from normal network configuration, or observed indications of MCA. The timing of planned CO should be determined based on a realistic assessment of their ability to create effects and support operations throughout the OE. This may require use of cyberspace capabilities in earlier phases of an operation than the use of capabilities that create physical effects. Effective planners and operators understand how other operations within the OE may impact the CO. For example, the joint force uses fire support coordination measures in air, land, and maritime operations to facilitate the rapid engagement of targets and simultaneously provide safeguards for friendly forces. CO deconfliction and coordination efforts with other operations should include similar measures.

b. **Deconfliction.** For CO, deconfliction is the act of coordinating the employment of cyberspace capabilities with applicable DOD, interagency, and multinational partners to ensure operations do not interfere, inhibit, or otherwise conflict with each other. The commander's intended effects in cyberspace, and the capabilities planned to create these effects, require deconfliction with other commands and agencies that may have equities in the same area of cyberspace. This critical step is managed from multiple aspects. From a purely technical perspective, it can be shown that two cyberspace capabilities can either interoperate without interference in the same environment or they cannot. However, from an operational risk perspective, even if multiple capabilities can operate without interference, it may not be wise to use them together. For example, the effect of one capability may draw the adversary's attention to the target system in a way that jeopardizes another previously unnoticed US or mission partner capability. Technical deconfliction uses the results of technical assurance evaluations and includes detailed interoperability analysis of each capability and the cyberspace aspects of the OE. CDRUSCYBERCOM is the DOD focal point for department and interagency deconfliction of all actions proposed for OCO and DCO-RA missions. Commander, JFHQ-DODIN, is the focal point for interagency deconfliction of global DODIN operations and DODIN DCO-IDM activities, which may affect more than one DOD component. The timelines required for analysis and coordination should be considered and included in the plan. Interagency coordination is often additive to DOD coordination and can extend overall preparation time. CO may also require deconfliction and synchronization with IJSTO. Information and processes related to IJSTO and its contribution to CO can be obtained from the IJSTO planners at CCMD or Service component HQs.

c. **EMS Factors**

(1) **EMS Dependencies.** Advancements in technology, including expansion of the IoT and the ever-increasing shift to mobile technologies, have progressively increased EMS complexity within the OE. This has significant implications for CO. The JFC uses a joint electromagnetic spectrum operations cell (JEMSOC) to coordinate elements of CO, space operations, electromagnetic warfare (EW), navigation warfare, various forms of EMS-dependent information collection, and C2. Although these activities can be integrated with other information activities as part of synchronizing OIE, the offensive aspects of CO, space operations, and EW operations are often conducted under different specific authorities. Likewise, some information activities enabled by CO, such as MISO and MILDEC, have their own execution approval process. Therefore, synchronizing information activities that use the EMS is a complex process that requires significant foresight and awareness of the various applicable policies. Planners should also maintain awareness of their operational dependencies on mobile devices and wireless networks, including cellular, wireless local area networks, Global Positioning System, and other

commercial and military uses of the EMS. Plans that assume access to the EMS for effects in cyberspace should consider contingencies for when bandwidth or interference issues preclude access to the required portion of the EMS.

(2) **Fires In and Through the EMS.** Cyberspace attack, EA, and offensive space operations are deconflicted through the JEMSOC to maximize the impact of each type of fires. Uncoordinated EA may significantly impact EMS-enabled cyberspace attack actions, and vice versa. Depending upon power levels, the geographic terrain in which they are used, and the nature of the system being targeted, unintended effects of EA and offensive space operations could also occur outside of a local commander's OA, just as higher-order effects of CO may be possible outside the OA. The JFC and staff may need to comply with different coordination requirements for the various types of fires that depend upon the EMS, forwarding requests for execution as early in the planning process as possible to comply with US law and to facilitate effective and timely effects. To minimize overlap, the primary responsibility for cyberspace attack coordination between USCYBERCOM and the joint force, including EMS-enabled cyberspace attack, occurs between the applicable JFHQ-C and CO-IPEs in coordination with the CCMD CO staff. Refer to respective doctrine and policy documents of supported information activities for specifics on their authorities.

See JP 3-85, Joint Electromagnetic Spectrum Operations, *and JP 3-14,* Joint Space Operations*, for more information on EMS factors.*

d. **Integration of Fires in Cyberspace.** In crisis and conflict, cyberspace attack capabilities, although they can be used in a stand-alone context, are generally most effective when integrated with other fires. Some examples of integrating fires are disruption of enemy air defense systems using EMS-enabled cyberspace attack; insertion of messages into enemy leadership's communications; degradation/disruption of enemy space-based and ground-based positioning, navigation, and timing systems; and disruption of enemy C2. Fires effects in cyberspace can be created at the strategic, operational, or tactical level, in any phase of the military operation, and coordinated with other fires to create maximum effect on target. Integrated fires are not necessarily simultaneous, since the timing of cyberspace attack effects may be most advantageous when placed before or after the effects of other fires. Each engagement presents unique considerations, depending upon the level and nature of the enemy's dependencies upon cyberspace. Supporting fires in cyberspace may be used in a minor role, or they can be a critical component of a mission when used to enable air, land, maritime, space, and special operations. Forces operating in the physical domains cannot use fires in cyberspace to best advantage unless they ensure synchronization of physical and virtual actions, clearly understand the type and timing of planned effects in cyberspace, and comprehensively assess cross-domain effects. Properly prepared and timed cyberspace attack can create effects that cannot be created any other way. Poorly timed fires in cyberspace can be useless, or even worse, interfere with an otherwise effective mission.

e. **Risk Concerns.** JFCs should continually seek to minimize risks to the joint force, as well as to friendly and neutral nations, societies, and economies, caused by use of cyberspace. Coordinated joint force operations benefit from the use of various cyberspace capabilities, including unclassified websites and Internet-hosted applications used for communication efforts with audiences internal and external to DOD. Forward-deployed forces use the Internet, mobile phones, and instant messaging for logistics and morale purposes, including communication with friends and family. These uses of cyberspace are targeted by myriad actors, from foreign nations to malicious insiders. The JFC works with JFHQ-DODIN and the Services, as well as with assigned cyberspace forces, to limit the threat to the DODIN and mission partners' cyberspace. Several areas of significant risk exist for the JFC:

(1) **Insider threats** are a significant concern to the joint force. Because insiders have a trusted relationship with access to the DODIN, the effects of their malicious or careless activity can be far more serious than those of external threats. Any user who does not closely follow cybersecurity policy can become an insider threat. Malicious insiders may exploit their access at the behest of foreign governments, terrorist groups, criminal elements, unscrupulous associates, or on their own initiative. Whether malicious insiders are committing espionage, making a political statement, or expressing personal disgruntlement, the consequences for DOD and national security can be devastating. JFCs use risk mitigation measures for this threat, such as consistently training the joint force to be alert for suspicious insider activity; use of two-person controls on particularly sensitive hardware, software, or data; and use of "zero trust" security models which treat all devices and users as suspicious and verify each request for access to data or services, regardless of from whom or where it originates.

(2) **Internet-based capabilities,** including e-mail, social networking, websites, and cloud-based repositories, are used for both official and unofficial purposes and pose continuously evolving security risks that are not fully understood. The security risks of Internet-based capabilities are often obscured, and our ability to mitigate these risks is limited, due to the commercial ownership of the majority of the supporting information systems or websites. These cyberspace and information security concerns, combined with bandwidth requirements of Internet applications, require the commander to be aware of and actively manage the impact of official and unofficial use of Internet-based capabilities.

(3) **Cross-domain (network) solutions** that connect systems operating at different classification levels can provide significant operational value to the JFC but complicate cryptographic and other security support considerations and should be included as a planning consideration. Cross-domain solutions are often required in multinational operations and at the tactical level. The pace of operations and increasing demand for information from commanders and their staffs can sometimes pressure end-users into using poor security practices. Likewise, emergent tasking for information sharing has sometimes caused network managers to build ad hoc links over existing commercial infrastructure or connect non-DOD US and partner cyberspace without adequate security controls. The security risk of these behaviors is significant. USCYBERCOM, through JFHQ-DODIN, works with JFCs to develop appropriate technical solutions and detailed security policies to address operational requirements without adding unnecessary risk. Planners should

include requirements for early coordination so the security features included are appropriate for the commander's needs.

7. Assessment of Cyberspace Operations

a. Assessment measures progress of the joint force toward mission accomplishment. Commanders continuously assess the OE and the progress of CO and compare them to their vision and intent. Measuring this progress toward the end state, and delivering timely, relevant, and reliable feedback into the planning process to adjust operations during execution, involves deliberately comparing the forecasted effects of CO with actual outcomes to determine the overall effectiveness of cyberspace force employment. More specifically, assessment is a commander-led activity that enables determination of progress toward attaining the desired end state, achieving objectives, or performing tasks. Commanders assess the risks of conducting specific CO against their expected effects. Common risks for CO external missions include detection of the activity, or the cyberspace capability being used, by a peer adversary, which could result in countermeasures that cause mission failure and heightened security at the target, co-option of the capability by the adversary for their own use, unintentional escalation, and attribution of CO activities to US forces.

b. The assessment process for CO external missions begins during planning and includes development and approval of measures of performance (MOPs) and measures of effectiveness (MOEs) of fires and other effects in cyberspace, as well as their contribution to the larger operation or objective. Timely assessment planning is required to ensure allocation of assessment resources and collection of pre-execution baseline information for later comparison. Historically, combat assessment has emphasized the battle damage assessment component of measuring physical and functional damage, but this approach does not always accurately characterize the entirety of an effect's impact, particularly with respect to CO. The effects of CO are often created outside the scope of battle and often do not create physical damage. Assessing the impact of effects of CO requires battle damage assessment analysis and assessment of physical, functional, and target system components. However, the higher-order effects of cyberspace actions are often subtle, and assessment of second- and third-order effects can be difficult. Therefore, assessment of fires in and through cyberspace frequently requires significant intelligence collection and analysis efforts. Incorporating pre-strike estimates and post-strike assessment for CO into the existing joint force staff processes increases the likelihood that all objectives are met.

c. **Assessment of CO at the Operational Level**

(1) The operational-level planner is concerned with the accumulation of tactical effects into an overall operational effect. At the operational level, planning and operations staffs develop objectives and desired effects for the JFC to assign to subordinates. Subordinate staffs use the assigned operational objectives to develop tactical-level objectives, tasks, and subordinate targeting objectives and effects and to plan tactical actions and associated MOPs/MOEs. Individual tactical actions typically combine with other tactical actions to create operational-level effects; however, they can have operational and strategic implications. Usually, the summation of tactical actions in an operational

theater is used to conduct an operational-level assessment, which in turn supports the strategic-level assessment (as required). Operational MOPs/MOEs avoid tactical information overload by providing commanders a shorthand method of tracking tactical actions and maintaining situational awareness. MOPs and MOEs are clearly definable and measurable, are selected to support and enhance the commander's decision process, and guide future actions that achieve objectives and attain end states.

(a) **MOEs.** MOEs are indicators used to measure a current system state, with change indicated by comparing multiple observations over time. MOEs are used to assess changes in targeted system behavior or in the OE. They measure progress toward the attainment of an end state, achievement of an objective, or creation of an effect. Data gathered on the target from its pre-mission state through access, execution, and possibly long-term post-operations analysis may enable later, more comprehensive assessment, including that of higher-order effects. MOEs generally reflect a trend or show progress toward or away from a measurable threshold. While MOEs may be harder to derive than MOPs for a discrete task, they are nonetheless essential to effective assessment. For example, a MOE for a cyberspace attack action might be a meaningful reduction in the throughput of enemy data traffic or their shift to a means of communication more vulnerable to interception. Assessment of CO takes place both inside and outside of cyberspace. For instance, a cyberspace attack to disrupt electric power might be assessed through visual observation to determine that the power is actually out.

(b) **MOPs.** MOPs are indicators used to measure a friendly action tied to measuring task accomplishment. MOPs are generally quantitative and are used in most aspects of combat assessment, which typically seeks specific quantitative data or a direct observation of an event to determine accomplishment of tactical tasks. An example of a MOP for a cyberspace exploitation action might be confirmation of gaining a required access or emplacing a cyberspace capability on a targeted system.

(2) Development of operational-level MOPs/MOEs for CO is still an emerging aspect of operational art. In some cases, activities in cyberspace alone have operational-level effects; for example, the use of a cyberspace attack to bring down or corrupt the enemy HQ network could very well reverberate through the entire JOA. A CO option may be preferable in some scenarios if its effects are temporary or reversible. In such cases, accurate assessment requires the ability to effectively track the current status of the potentially changing effect using MOE indicators.

(3) CO often involve multiple commanders. Additionally, with CO typically conducted as part of a larger operation, assessment of CO is usually done in the context of supporting the overarching objectives. Therefore, CO assessments require close coordination within each staff and across multiple commands. Coordination and federation of the assessment efforts may require prior arrangements before execution. CO planners should submit assessment requests as early as possible and provide sufficient justification to support priority allocation of relevant collection capabilities, including those outside of cyberspace.

See JP 5-0, Joint Planning, *for a detailed description of assessment. See JP 3-60,* Joint Targeting, *and Defense Intelligence Agency Publication 2820-4-03,* Battle Damage Assessment (BDA) Quick Guide, *for more information on the assessment process related to targeting, battle damage assessment, and munitions effectiveness assessment.*

8. Interorganizational Considerations

a. When appropriate, JFCs coordinate and integrate their CO with interagency partners during planning and execution. Effective integration of interagency considerations is vital to successful military operations, especially when the joint force conducts shaping, stabilization, and transition to civil authority activities. Just as JFCs and their staffs consider how the capabilities of other USG departments and agencies and NGOs can assist in accomplishing military missions and achieving broader national strategic objectives, JFCs should also consider the capabilities and priorities of interagency partners in planning and executing CO. In collaboration with interagency representatives, the JS, and USCYBERCOM, JFCs should coordinate with interagency partners during CO planning to help ensure appropriate agreements exist to support their plans and to leverage all available instruments of national power.

b. At the national level, the National Security Council, with its interagency policy committees and interagency working groups, advises and assists the President on all aspects of national security policy. OSD and the JS, in consultation with the Services and CCMDs, coordinate interagency support required to support the JFC's plans and orders. While supported CCDRs are the focal points for interagency coordination in support of operations in their AORs, interagency coordination with supporting commanders is also important. For integration into their operational-level estimates, plans, and operations, commanders should only consider interagency cyberspace capabilities and capacities that interagency partners can realistically commit to the effort.

c. Military leaders work with the other members of the national security team to promote unified action. A number of factors can complicate the coordination process, including various agencies' different and sometimes conflicting policies, overlapping legal authorities, roles and responsibilities, procedures, and decision-making processes for CO. Interagency coordination factors typically derive from national leadership direction or from authorities such as US law. By identifying and understanding these equities early, DOD may expedite the planning process, identify additional courses of action, or reduce operational risk. A supported commander develops interagency coordination requirements and mechanisms for each contingency plan. The JFC's staff requires a clear understanding of military cyberspace capabilities, requirements, operational limitations, liaison, and legal considerations. Additionally, planners should understand the nature of this relationship and the types of CO support interagency partners can provide. In the absence of an interagency command structure, JFCs are required to build consensus to achieve unity of effort. Robust liaison facilitates understanding, coordination, and mission accomplishment.

d. Interagency leadership relationships, lines of authority, and planning processes vary greatly from those of DOD. Interagency management techniques often involve committees, steering groups, and/or interagency working groups organized along functional lines. During joint operations, use of a JIACG provides the CCDR and subordinate JFCs with an increased capability to coordinate with other USG departments and agencies. The JIACG is composed of USG civilian and military experts tailored to meet the CCDR's specific needs and accredited to the CCDR. The JIACG establishes regular, timely, and collaborative working relationships between civilian and military planners, providing a CCDR with the capability to collaborate at the operational level with other USG departments and agencies. JIACG members participate in all appropriate planning efforts. Additionally, they provide a collaborative conduit back to their parent organizations to help synchronize joint operations with the efforts of nonmilitary organizations. In the absence of a JIACG focused on CO, planners may find it more difficult to verify that all mission partner equities in cyberspace are accounted for and, therefore, should begin to develop contacts with relevant departments and agencies as soon as the planning process begins.

9. Multinational Considerations

a. Collective security is a strategic objective of the United States, and joint planning is frequently accomplished within the context of planning for multinational operations. Despite the potential for increased risk inherent in relying on others, the complexity of cyberspace and the enormous variety of its threats means the United States does rely on partnerships to protect its cyberspace and to achieve CO external mission objectives. There is no single doctrine for multinational action, and each alliance or coalition develops its own protocols and plans. US planning for joint operations accommodates and complements such protocols and plans for potential use of US cyberspace forces to protect MNF networks. JFCs also anticipate and incorporate mission partner planning factors, such as their domestic laws, regulations, and operational limitations on the use of various cyberspace capabilities and tactics.

b. When working within an MNF, each nation and Service can expect to be tasked by the commander with the mission(s) most suited to their particular capability and capacity. For example, a CPT supporting a CCMD could be tasked, with the agreement of all nations involved, to investigate and mitigate the effects of MCA on a multinational network. The USCYBERCOM focus on defending forward and engaging threats before they reach US cyberspace makes these DCO-IDM missions a priority activity that has the potential to improve both US and partner readiness and resilience in cyberspace. CO planning, coordination, and execution items that require consideration when developing an MNF operation or campaign plan include:

(1) National agendas of the PNs on an MNF may differ significantly from those of the United States, creating potential difficulties in agreeing on CO objectives.

(2) Differing national standards and foreign laws, as well as interpretation of international laws pertaining to operations in cyberspace, may affect their ability to participate in certain CO. These differences may result in partner policies or capabilities that are either narrower or broader than those of the United States.

(3) Nations without established CO doctrine may need to be advised of the potential benefits of CO and assisted in integrating CO into the planning process.

(4) Nations in an MNF often require approval for the CO portion of plans and orders from higher authority, which may impede CO implementation. This national-level approval requirement increases potential constraints and restraints upon the participating national forces and further lengthens the time required to gain approval for their participation. Commanders and planners should be proactive in seeking to understand PNs' laws, policies, and other matters that might affect their use of CO and anticipate the additional time required for approval through parallel national command structures. Partners' national caveats and ROE are often not transmitted thoroughly to commanders and planners, potentially leading to misunderstanding, delays, and incompleteness in execution.

(5) Security restrictions may prevent full disclosure of individual CO plans and orders between multinational partners; this may complicate CO synchronization efforts. Therefore, the JFC's staff should seek approval for sharing required information among partners and then issue specific guidance on the release of classified US material to the MNF as early as possible during planning. Likewise, once these information-sharing restrictions are identified by each nation, policy should be established and mechanisms put in place to encourage appropriate CO-related information sharing across the force. These considerations further highlight the importance of ensuring CO material is not over classified and is releasable to partners to the greatest extent possible.

(6) To effectively conduct multinational operations, mission partners require appropriate access to systems, services, and information. Emerging standards for the technologies and applications applied to DODIN segments used in a joint environment are designed to allow seamless and secure interaction with multinational partners. Until such technology is widespread, the US joint force strives to provide necessary and appropriate access and support at the lowest appropriate security classification level on the infrastructure they have available. Commanders involved in multinational operations can enable this shared access by coordinating with proper authorities early to determine appropriate access levels, necessary services, and satisfactory means for expediting the process for foreign disclosure of appropriate intelligence information consistent with *National Disclosure Policy*, and Director of National Intelligence guidance, as applicable. Hardware and software incompatibilities can still be expected and may cause a slowdown in the sharing of information among multinational partners. Failure to bridge these incompatibilities may introduce seams, gaps, and vulnerabilities requiring additional cyberspace security and defense efforts.

(7) Responsibility for cyberspace security and cyberspace defense actions to protect multinational networks should be made clear before the network is activated. If responsibility for these actions is to be shared among PNs, explicit agreements, including expectations and limitation of action of each partner, should be in place. Unless otherwise agreed, US cyberspace forces or other DOD personnel protect DODIN segments of multinational networks.

c. **Integration.** In support of each MNF, an established hierarchy of bilateral or multilateral bodies defines objectives, develops strategies, and coordinates strategic guidance for planning and executing multinational operations, including CO. Through dual involvement in national and multinational security processes, USG leaders integrate national and theater strategic CO planning with the MNF whenever possible. Within the multinational structure, US participants work to ensure objectives and strategy complement US interests and are compatible with US capabilities. Within the US national structure, US participants verify that international commitments are reflected in national military strategy and are adequately addressed in strategic guidance for joint planning. Planning with international organizations and NGOs is often necessary, particularly if CO support foreign humanitarian assistance, peace operations, and other stabilization efforts. Incorporating NGOs and their capabilities into the planning process requires the JFC and staff to balance NGOs' information requirements with the organizations' need to know. Additionally, many NGOs are hesitant to become associated with military organizations in any form of formal relationship, especially in the case of conducting CO, because doing so could compromise their status as an independent entity, restrict their freedom of movement, and even place their members at risk in uncertain or hostile environments.

d. Multinational partners often use different lexicons, assumptions, decision thresholds, and operational limitations for CO. All of these factors affect coordination, integration, and execution and should be taken into consideration during planning.

See JP 3-16, Multinational Operations, *for more information on multinational operations.*

Intentionally Blank

APPENDIX A
(U) CLASSIFIED PLANNING CONSIDERATIONS FOR JOINT CYBERSPACE OPERATIONS
(PUBLISHED SEPARATELY)

Intentionally Blank

APPENDIX B
REFERENCES

The development of JP 3-12 is based upon the following primary references:

1. General

a. Title 10, USC.

b. Title 32, USC.

c. Title 50, USC.

d. Executive Order 12333, *US Intelligence Activities,* as amended.

e. Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.*

f. Executive Order 14028, *Improving the Nation's Cybersecurity*.

g. National Security Memorandum-8, *Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems.*

h. Homeland Security Presidential Directive-5, *Management of Domestic Incidents.*

i. National Security Presidential Memorandum-13, *(U) United States Cyber Operations Policy,* as amended.

j. PPD-21, *Critical Infrastructure Security and Resilience.*

k. PPD-41, *United States Cyber Incident Coordination.*

l. *Trilateral Memorandum of Agreement Among the Department of Defense and the Department of Justice and the Intelligence Community Regarding Computer Network Attack and Computer Network Exploitation Activities,* 9 May 2007.

m. *National Policy Governing the Release of Information Systems Security (INFOSEC) Products or Associated INFOSEC Information to Foreign Governments.*

n. National Security Presidential Directive-54/Homeland Security Presidential Directive-23, *Cybersecurity Policy.*

o. National Security Directive 42, *National Policy for the Security of National Security Telecommunications and Information Systems.*

p. *Memorandum of Agreement Between the Department of Defense and The Department of Homeland Security Regarding Department of Defense and US Coast Guard Cooperation on Cybersecurity and Cyberspace Operations,* 27 September 2010.

q. *National Infrastructure Protection Plan.*

r. *Unified Command Plan*, 2021.

2. Department of Defense Publications

a. *(U) National Military Strategy of the United States of America, 2022.*

b. *The Department of Defense Cyber Strategy.*

c. *Department of Defense Strategy for Operating in the Information Environment.*

d. Deputy Secretary of Defense Memorandum, *Policy for Department of Defense (DOD) Interactive Internet Activities,* June 8, 2007.

e. *(U) Global Force Management Allocation Plan.*

f. *(U) Global Force Management Implementation Guidance.*

g. *Defense Strategic Guidance.*

h. DODD 2311.01, *DOD Law of War Program.*

i. DODD 3020.40, *Mission Assurance (MA).*

j. DODD 3025.18, *Defense Support of Civil Authorities (DSCA).*

k. DODD 3600.01, *Information Operations (IO).*

l. DODD 5100.20, *National Security Agency/Central Security Service (NSA/CSS).*

m. DODD 5143.01, *Under Secretary of Defense for Intelligence and Security (USD[I&S]).*

n. DODD 5205.15E, *DOD Forensic Enterprise (DFE).*

o. DODD 5505.13E, *DOD Executive Agent (EA) for the DOD Cyber Crime Center (DC3).*

p. DODD 8000.01, *Management of the Department of Defense Information Enterprise (DOD IE).*

q. DODI O-3600.03, *Testing and Evaluation of Cyberspace Effects and Enabling Capabilities.*

r. DODI 3607.02, *Military Information Support Operations (MISO).*

s. DODI 5205.13, *Defense Industrial Base (DIB) Cybersecurity (CS) Activities.*

t. DODI 8500.01, *Cybersecurity.*

u. DODI 8520.02, *Public Key Infrastructure (PKI) and Public Key (EK) Enabling.*

v. DODI 8530.01, *Cybersecurity Activities Support to DOD Information Network Operations.*

w. DODI 8531.01, *DOD Vulnerability Management.*

x. DODI 8560.01, *Communications Security (COMSEC) Monitoring.*

y. Directive-Type Memorandum 17-007, *Interim Policy and Guidance for Defense Support to Cyber Incident Response,* June 21, 2017, incorporating Change 4, May 21, 2021.

z. *Department of Defense Law of War Manual.*

aa. Defense Intelligence Agency Publication 2820-4-03, *Battle Damage Assessment (BDA) Quick Guide.*

3. Chairman of the Joint Chiefs of Staff Publications

a. CJCSI 3100.01E, *Joint Strategic Planning System.*

b. CJCSI 3121.01B, *(U) Standing Rules of Engagement/Standing Rules for the Use of Force for US Forces.*

c. CJCSI 3210.01C, *Joint Information Operations Proponent.*

d. CJCSI 3370.01C, *Target Development Standards.*

e. CJCSI 5810.01D, *Implementation of the DOD Law of War Program.*

f. CJCSM 3105.01A, *Joint Risk Analysis Methodology.*

g. CJCSM 3122.07A, *Integrated Joint Special Technical Operations (IJSTO) Supplement to Joint Operation Planning and Execution System (JOPES),* Volume I *(Planning, Policies, and Procedures).*

h. CJCSM 3130.06C, *(U) Global Force Management Allocation Policies and Procedures.*

i. CJCSM 3130.08, *(U) IJSTO Supplement to CJCSM 3130.03 Planning and Execution Formats.*

j. CJCSM 3139.01, *(U) Review and Approval Process for Cyberspace Operations.*

k. CJCSM 3314.01A, *Intelligence Planning.*

l. CJCSM 6510.01B, *Cyber Incident Handling Program.*

m. CJCS 041530Z December 2020, *EXORD to Implement Cyberspace Operations C2 Framework,* Revision 1 *Command and Control Framework.*

n. JP 1, Volume 1, *Joint Warfighting.*

o. JP 2-0, *Joint Intelligence.*

p. JP 3-0, *Joint Campaigns and Operations.*

q. JP 3-04, *Information in Joint Operations.*

r. JP 3-07, Joint *Stabilization Activities.*

s. JP 3-08, *Interorganizational Cooperation.*

t. JP 3-13.2, *Military Information Support Operations.*

u. JP 3-13.3, *Operations Security.*

v. JP 3-13.4, *Military Deception.*

w. JP 3-14, *Joint Space Operations.*

x. JP 3-16, *Multinational Operations.*

y. JP 3-25, *Joint Countering Threat Networks.*

z. JP 3-27, *Homeland Defense.*

aa. JP 3-28, *Defense Support of Civil Authorities.*

bb. JP 3-60, *Joint Targeting.*

cc. JP 3-61, *Public Affairs.*

dd. JP 3-84, *Legal Support.*

ee. JP 3-85, *Joint Electromagnetic Spectrum Operations.*

ff. JP 5-0, *Joint Planning.*

gg. JP 6-0, *Joint Communications System.*

Intentionally Blank

APPENDIX C
ADMINISTRATIVE INSTRUCTIONS

1. User Comments

Users in the field are highly encouraged to submit comments on this publication using the Joint Doctrine Feedback Form located at: https://jdeis.js.mil/jdeis/jel/jp_feedback_form.pdf and e-mail it to: js.pentagon.j7.mbx.jedd-support@mail.mil. These comments should address content (accuracy, usefulness, consistency, and organization), writing, and appearance.

2. Authorship

a. The lead agent for this publication is USCYBERCOM, and the Joint Staff doctrine sponsor for this publication is the Director for Operations (J-3).

b. The following staff, in conjunction with the joint doctrine development community, made a valuable contribution to the revision of this joint publication: lead agent, Mr. Paul Schuh, USCYBERCOM; Joint Staff doctrine sponsor, CDR William Wilson and LCDR Ryan Seligman, Joint Staff J-39; Mr. Gerald Belliveau, Joint Staff J-7, Joint Doctrine Analysis Branch; and LTC Travis Hacker, Joint Staff J-7, Joint Doctrine Branch.

3. Supersession

This publication supersedes JP 3-12, *Cyberspace Operations,* 08 June 2018.

4. Change Recommendations

a. To provide recommendations for urgent and/or routine changes to this publication, please complete the Joint Doctrine Feedback Form located at: https://jdeis.js.mil/jdeis/jel/jp_feedback_form.pdf and e-mail it to: js.pentagon.j7.mbx.jedd-support@mail.mil.

b. When a Joint Staff directorate submits a proposal to the CJCS that would change source document information reflected in this publication, that directorate will include a proposed change to this publication as an enclosure to its proposal. The Services and other organizations are requested to notify the Joint Staff J-7 when changes to source documents reflected in this publication are initiated.

5. Lessons Learned

The Joint Lessons Learned Program's (JLLP's) primary objective is to enhance joint force readiness and effectiveness by contributing to improvements in doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy. The Joint Lessons Learned Information System (JLLIS) is the DOD system of record for lessons learned and facilitates the collection, tracking, management, sharing, collaborative resolution, and dissemination of observations, issues, best practices, and lessons learned to improve the development and readiness of the joint force. The JLLP integrates with joint doctrine through the joint doctrine development process by providing insights and lessons learned derived from operations, exercises, war games, and other events. As these inputs are incorporated into joint doctrine, they become institutionalized for future use, a major goal of the JLLP. Insights and lessons learned are routinely sought and incorporated into draft JPs throughout formal staffing of the development process. The JLLIS Website can be found at https://www.jllis.mil (NIPRNET) or http://www.jllis.smil.mil (SIPRNET).

6. Releasability

LIMITED. This JP is approved for limited release. The authors of this publication have concluded that information in this publication should be disseminated on an as-needed basis and is limited to common access card holders. Requests for distribution to non-common access card holders should be directed to the Joint Staff J-7.

7. Printing and Distribution

Before distributing this JP, please e-mail the Joint Staff J-7, Joint Doctrine Branch, at js.pentagon.j7.mbx.jedd-support@mail.mil, or call 703-692-7273/DSN 692-7273, or contact the lead agent or Joint Staff doctrine sponsor.

a. The Joint Staff does not print hard copies of JPs for distribution. An electronic version of this JP is available on:

(1) NIPRNET Joint Electronic Library Plus (JEL+) at https://jdeis.js.mil/jdeis/index.jsp (limited to .mil and .gov users with a DOD common access card) and

(2) SIPRNET JEL+ at https://jdeis.js.smil.mil/jdeis/index.jsp.

b. Access to this unclassified publication is limited. This JP can be locally reproduced for use within the combatant commands, Services, National Guard Bureau, Joint Staff, and combat support agencies. However, reproduction authorization for this JP must be IAW lead agent/Joint Staff doctrine sponsor guidance.

GLOSSARY
PART I—SHORTENED WORD FORMS (ABBREVIATIONS, ACRONYMS, AND INITIALISMS)

AOR	area of responsibility
C2	command and control
CCDR	combatant commander
CCMD	combatant command
CCMF	Cyber Combat Mission Force
CDRUSCYBERCOM	Commander, United States Cyber Command
CDRUSSPACECOM	Commander, United States Space Command
CI	counterintelligence
CI/KR	critical infrastructure and key resources
CIO	chief information officer
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff instruction
CJCSM	Chairman of the Joint Chiefs of Staff manual
CMF	Cyber Mission Force
CMT	combat mission team
CNMF	Cyber National Mission Force
CNMF-HQ	Cyber National Mission Force-Headquarters
CO	cyberspace operations
COCOM	combatant command (command authority)
CO-IPE	cyberspace operations-integrated planning element
CONOPS	concept of operations
COP	common operational picture
CPF	Cyber Protection Force
CPT	cyberspace protection team
CSA	combat support agency
CSSP	cybersecurity service provider
CST	combat support team
DACO	directive authority for cyberspace operations
DC3	Department of Defense Cyber Crime Center
DCI	defense critical infrastructure
DCO	defensive cyberspace operations
DCO-IDM	defensive cyberspace operations-internal defensive measures
DCO-RA	defensive cyberspace operations-response actions
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DIB	defense industrial base
DISA	Defense Information Systems Agency
DOD	Department of Defense
DODD	Department of Defense directive
DODI	Department of Defense instruction

DODIN	Department of Defense information network
DOJ	Department of Justice
DSCA	defense support of civil authorities
EA	electromagnetic attack
EEI	essential element of information
EMS	electromagnetic spectrum
EW	electromagnetic warfare
EXORD	execute order
FBI	Federal Bureau of Investigation (DOJ)
GFMAP	Global Force Management Allocation Plan
GFMIG	Global Force Management Implementation Guidance
HFO	hunt forward operations
HQ	headquarters
IAW	in accordance with
IC	intelligence community
IE	information environment
IGL	intelligence gain/loss
IJSTO	integrated joint special technical operations
IoT	Internet of Things
IP	Internet protocol
ISP	Internet service provider
ISR	intelligence, surveillance, and reconnaissance
IT	information technology
JEMSOC	joint electromagnetic spectrum operations cell
JFC	joint force commander
JFHQ	joint force headquarters
JFHQ-C	joint force headquarters-cyberspace
JFHQ-DODIN	Joint Force Headquarters-Department of Defense Information Network
JIACG	joint interagency coordination group
JOA	joint operations area
JP	joint publication
JPP	joint planning process
JS	Joint Staff
JTF	joint task force
JTL	joint target list
LE	law enforcement
MCA	malicious cyberspace activity

MILDEC	military deception
MISO	military information support operations
MNF	multinational force
MOE	measure of effectiveness
MOP	measure of performance
MRT-C	mission-relevant terrain in cyberspace
NC3	nuclear command, control, and communications
NG	National Guard
NGO	nongovernmental organization
NIPRNET	Nonclassified Internet Protocol Router Network
NMT	national mission team
NST	national support team
OA	operational area
OCO	offensive cyberspace operations
OE	operational environment
OIE	operations in the information environment
OPCON	operational control
OPORD	operation order
OPSEC	operations security
OSD	Office of the Secretary of Defense
OSINT	open-source intelligence
PIR	priority intelligence requirement
PIT	platform information technology
PN	partner nation
PPD	Presidential policy directive
RC	Reserve Component
RFI	request for information
ROE	rules of engagement
SATCOM	satellite communications
SCC	Service cyberspace component
SecDef	Secretary of Defense
SIGINT	signals intelligence
SIPRNET	SECRET Internet Protocol Router Network
TST	time-sensitive target
US	United States
USC	United States Code
USCYBERCOM	United States Cyber Command
USG	United States Government
USTRANSCOM	United States Transportation Command

PART II—TERMS AND DEFINITIONS

1. JP 3-12, *Joint Cyberspace Operations,* 19 December 2022, Active Terms and Definitions

cyber-persona. The combined features comprising the digital representation of an actor or entity in cyberspace used for intelligence analysis and reporting and for planning operations related to that entity. (Approved for inclusion in the DOD Dictionary.)

cyberspace. A global domain within the information environment consisting of the interdependent networks of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (DOD Dictionary. Source: JP 3-12)

cyberspace attack. Actions taken in and through cyberspace that create denial (i.e., degradation, disruption, or destruction) or manipulation effects in cyberspace and are considered a form of fires. (Approved for incorporation into the DOD Dictionary.)

cyberspace capability. A device or computer program, including any combination of software, firmware, or hardware, designed to create an effect in or through cyberspace. (DOD Dictionary. Source: JP 3-12)

cyberspace defense. Actions taken within protected cyberspace to defeat specific threats that have breached or are threatening to breach cyberspace security measures. (Approved for incorporation into the DOD Dictionary.)

cyberspace exploitation. Actions taken in cyberspace to gain intelligence, maneuver, collect information, or perform other enabling actions required to prepare for future military operations. (DOD Dictionary. Source: JP 3-12)

cyberspace security. Actions taken within protected cyberspace to prevent unauthorized access to, exploitation of, or damage to computers and networks, including platform information technology. (Approved for incorporation into the DOD Dictionary.)

cyberspace superiority. The degree of dominance in cyberspace by one force that permits the secure, reliable conduct of operations by that force and its related land, air, maritime, and space forces at a given time and place without prohibitive interference. (DOD Dictionary. Source: JP 3-12)

cyberspace system operation. Actions taken within the Department of Defense information network to ensure it operates in support of its user’s mission, including all non-security actions to administer, configure, update, extended, maintain, or repair it. (Approved for inclusion in the DOD Dictionary.)

defensive cyberspace operations. Missions to preserve the ability to utilize and protect blue cyberspace capabilities and data by defeating on-going or imminent malicious cyberspace activity. Also called **DCO.** (Approved for incorporation into the DOD Dictionary.)

defensive cyberspace operations-internal defensive measures. A defensive cyberspace operations mission in which defense actions occur within the defended portion of cyberspace. Also called **DCO-IDM.** (Approved for incorporation into the DOD Dictionary.)

defensive cyberspace operations-response actions. A defensive cyberspace operations mission executed external to the defended network or portion of cyberspace without the permission of the owner of the affected system. Also called **DCO-RA.** (Approved for incorporation into the DOD Dictionary.)

Department of Defense information network operations. Operations to secure, configure, operate, extend, maintain, and sustain Department of Defense cyberspace to create and preserve the confidentiality, availability, and integrity of the Department of Defense information network. Also called **DODIN operations.** (DOD Dictionary. Source: JP 3-12)

directive authority for cyberspace operations. The authority to issue orders and directives to all Department of Defense components to execute global Department of Defense information network operations and defensive cyberspace operations internal defensive measures. Also called **DACO.** (DOD Dictionary. Source: JP 3-12)

expeditionary cyberspace operations. Cyberspace operations that require the deployment of cyberspace forces within the physical domains. (Approved for inclusion in the DOD Dictionary.)

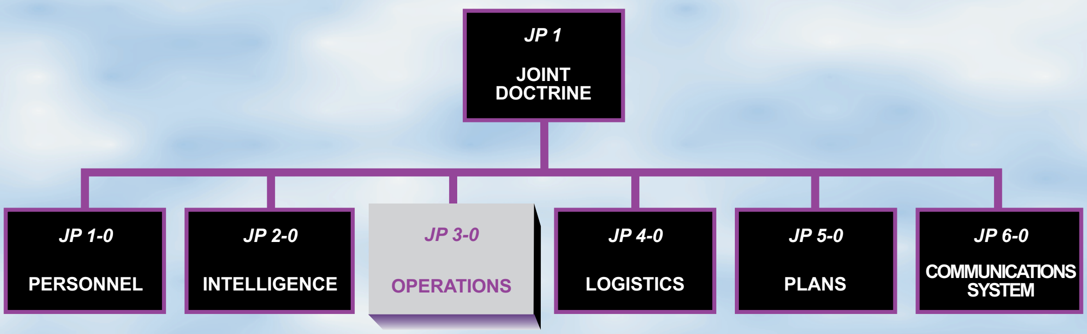
offensive cyberspace operations. Missions intended to project power in and through cyberspace. Also called **OCO.** (DOD Dictionary. Source: JP 3-12)

2. Terms Removed from the DOD Dictionary

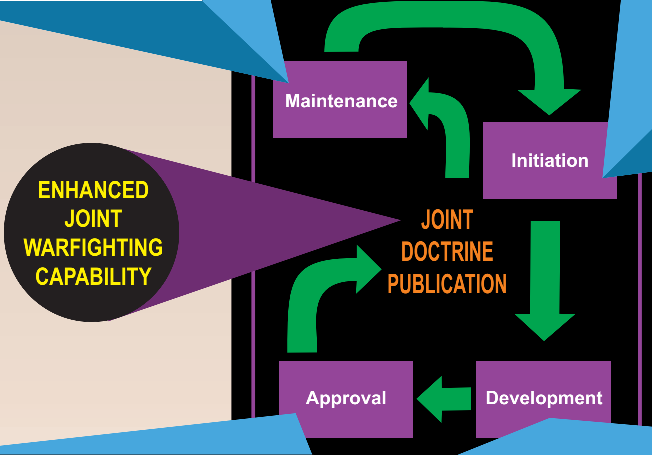
- **Supersession of JP 3-12, *Cyberspace Operations,* 08 June 2018:** no terms removed.

Intentionally Blank

JOINT DOCTRINE PUBLICATIONS HIERARCHY



All joint publications are organized into a comprehensive hierarchy as shown in the chart above. **Joint Publication (JP) 3-12** is in the **Operations** series of joint doctrine publications. The diagram below illustrates an overview of the development process:


Maintenance
Initiation
ENHANCED JOINT WARFIGHTING CAPABILITY
JOINT DOCTRINE PUBLICATION
Approval
Development

STEP #1 - Initiation

- Joint doctrine development community (JDDC) submission to fill extant operational void
- Joint Staff (JS) J-7 conducts front-end analysis
- Joint Doctrine Planning Conference validation
- Program directive (PD) development and staffing/joint working group
- PD includes scope, references, outline, milestones, and draft authorship
- JS J-7 approves and releases PD to lead agent (LA) (Service, combatant command, JS directorate)

STEP #2 - Development

- LA selects primary review authority (PRA) to develop the first draft (FD)
- PRA develops FD for staffing with JDDC
- FD comment matrix adjudication
- JS J-7 produces the final coordination (FC) draft, staffs to JDDC and JS via Joint Staff Action Processing (JSAP) system
- Joint Staff doctrine sponsor (JSDS) adjudicates FC comment matrix
- FC joint working group

STEP #3 - Approval

- JSDS delivers adjudicated matrix to JS J-7
- JS J-7 prepares publication for signature
- JSDS prepares JS staffing package
- JSDS staffs the publication via JSAP for signature

STEP #4 - Maintenance

- JP published and continuously assessed by users
- Formal assessment begins 24-27 months following publication
- Revision begins 3.5 years after publication
- Each JP revision is completed no later than 5 years after signature

JOINT CHIEFS OF STAFF